Heidelberger Texte zur Mathematikgeschichte

Autor: **Landsberg, Georg** (1865–1912)

Titel: **Untersuchungen über die Theorie der Ideale**

Diss.-Vermerk: Breslau, Phil. Fak., Inaug.-Diss v. 29. März 1890

Signatur UB Heidelberg: Z 1085,4

Die Dissertation enhält auf der letzten Seite die Thesen und auf der vorletzten einen Lebenslauf in lateinischer Sprache.

4

Untersuchungen

über die

Theorie der Ideale.

Inaugural-Dissertation

welche mit Genehmigung

der hohen philosophischen Facultät der Universität Breslau

zur Erlangung der Doctorwürde

am Sonnabend, den 29. März 1890, Vormittags 11 Uhr

in der Aula Leopoldina

gegen die Herren Opponenten:

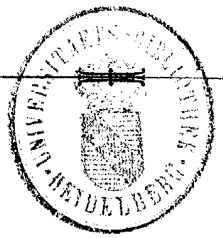
Dr. phil. Max Hamburger,
Assistent am physikalischen Institut der Universität Breslau

Dr. phil. Hans Seger

öffentlich vertheidigen wird

Georg Landsberg

aus Breslau.



Breslau

Druck von G. Hoyer & Comp.

Meinen lieben Eltern

gewidmet.

Einleitung.

Seitdem Gauss in seiner berühmten zweiten Abhandlung über die biquadratischen Reste (1832) die ganzen complexen Zahlen in die Arithmetik eingeführt hat, ist das Problem der Herstellung möglicher Zahlentheorieen in höheren Bereichen nicht mehr zum Stillstand gekommen. Aber der Lösung dieses Problems, welche sich in dem von Gauss betrachteten Gebiete verhältnissmässig mit Leichtigkeit vollzog, sobald einmal der an sich überaus merkwürdige Gedanke, in der Zahlentheorie über die rationalen Zahlen hinauszugehen, gefasst war, stellten sich bei allgemeinerer Untersuchung unerwartet grosse Schwierigkeiten entgegen, welche den Mathematikern fast unüberwindlich erscheinen mussten. Diese Schwierigkeiten bestanden — kurz gesagt — darin, dass die unzerlegbaren ganzen Zahlen eines endlichen Körpers die Primzahleigenschaft verloren; Primzahleigenschaft spricht man aber einer ganzen Zahl zu, wenn aus der Annahme, dass sie ein Product zweier ganzer Zahlen theilt, gefolgert werden darf, dass sie einen der beiden Factoren dieses Productes theilt. Legte man also den Complex der ganzen Zahlen eines endlichen Körpers der Untersuchung zu Grunde, so erhielt man zwar beschränkte Zerlegbarkeit in diesem so begrenzten Gebiete, aber die Eindeutigkeit der Zerlegung kam im allgemeinen in Wegfall, und damit fiel die Möglichkeit, eine Zahlentheorie in solchen Körpern aufzubauen.

Kummers unvergessliche Leistung ist es, den Pfad in diesem unwegsam scheinenden Gebiete gefunden zu haben. Durch die Schöpfung der idealen Zahlen gelang es ihm, im Bereiche der Kreistheilungskörper die Schwierigkeiten zu heben und die Gesetze der Theilbarkeit aufs glücklichste wiederherzustellen.*)

So glänzend die Kummer'sche Entdeckung war, so bot doch die Verallgemeinerung des Begriffes der idealen Zahl, wie sie zur Lösung des allgemeinsten Problemes dieser Art erforderlich wurde, immer noch bedeutende Schwierigkeiten dar. Die Kummer'sche ideale Zahl hat nämlich die charakteristische Eigenthümlichkeit, dass nicht die ideale Zahl selbst, sondern dass die Theilbarkeit durch die ideale Zahl und zwar durch Congruenzen definirt wird.**) Lag hierin an sich schon ein die Theorie der idealen Zahlen sehr wesentlich erschwerendes Moment, so trat noch ein anderes und grösseres Hemmniss hinzu: die Definition der idealen Zahl durch Congruenzen verdankt nämlich ihre Möglichkeit bloss dem glücklichen Umstande, dass die sämmtlichen ganzen Zahlen eines Kreistheilungskörpers als ganze, rationale und ganzzahlige Functionen einer von ihnen dargestellt werden können; es giebt aber Körper, für welche die in ihnen enthaltenen ganzen Zahlen sich nicht alle als ganze ganzzahlige Functionen einer von ihnen ausdrücken lassen, und diese setzen der Definition der idealen Zahl durch Congruenzen einen, wie es scheint, unüberwindlichen Widerstand entgegen.***)

Die genannten Umstände haben Herrn Dedekind bei seinen langjährigen rastlosen Bemühungen um das Problem

*) Kummers wichtigste Arbeiten hierüber sind: Crelles Journal Bd. 30, 35, 40, 53; Abhandlungen der Berliner Akademie 1856, 1857, 1859, 1861, und die zusammenfassende Darstellung (1851) des Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers in Liouvilles Journal Bd. 16 p. 377—498.

**) Damit steht es nicht in Widerspruch, dass Kummer den Satz ausspricht, dass jede ideale Zahl als Wurzel einer wirklichen Zahl dargestellt werden kann. Liouville l. c. p. 445.

***) Dedekind, Göttinger Anzeiger vom 20. Sept. 1871; Göttinger Abhandlungen Bd. 23, 1878 und der zu dieser Abhandlung gehörige Aufsatz in Crelles Journ. Bd. 54.

der idealen Zahlen dazu veranlasst, die alten Principien fallen zu lassen und die Theorie der ganzen Zahlen eines Körpers auf eine neue Basis zu stellen, deren Wesen darin besteht, dass an die Stelle der idealen Zahl der rein speculative Begriff des Ideals gesetzt wird. Der Begriff des Ideals tritt zu dem der idealen Zahl in die enge Beziehung, dass er die Gesammtheit aller durch eine und dieselbe, wirkliche oder ideale, Zahl theilbaren wirklichen Zahlen bedeutet. Durch consequente Verfolgung der Operationen, welche man mit solchen Systemen von Zahlen vornehmen kann, und durch scharfsinnige Ermittelung des analytischen Inhaltes, welcher den auftretenden algebraischen Gebilden innewohnt, gelangt Herr Dedekind dazu, für die Ideale eine jedesmalige und ganz bestimmte Zerlegung nachzuweisen, welche der Zerlegung der Zahlen in Primfactoren vollkommen parallel verläuft. Die Theorie der höheren Congruenzen ist alsdann nicht mehr Grundlage, sondern ein blosses Hilfsmittel zur analytischen Fixirung der durch die Theorie der Ideale statuirten Begriffe. Diese Principien hat Herr Dedekind zuerst sehr kurz in der zweiten Auflage der Dirichlet'schen Zahlentheorie (1871) und sodann in ausführlicherer Darstellung in zwei ausgezeichneten Abhandlungen publicirt.*)

Aus dem Studium dieser Dedekind'schen Untersuchungen ist die vorliegende Arbeit im wesentlichen erwachsen; sie beabsichtigt, im Anschluss an dieselben einmal den Begriff der idealen Zahl, welcher bei Herrn Dedekind fast ganz in den Hintergrund tritt, etwas näher zu determiniren und sodann den von Herrn Dedekind nur angegebenen Satz zu beweisen, dass mit den Idealen eines Normalkörpers auch die Ideale jedes Divisors dieses Normalkörpers bekannt sind. Zu letzterem Zwecke erschien es erforderlich, die

*) 1. Sur la théorie des nombres entiers algébriques. Paris 1877; Separatabdruck aus dem Bulletin des Sciences math. et astron. réd. par Darboux, Hoüel et Tannery; 1. sér. t. XI p. 278—288; 2. sér. t. I p. 17—41, p. 69—92, p. 144—164, p. 207—248. 2. Letztes Supplement der dritten Auflage der Dirichlet'schen Zahlentheorie. (Braunschweig 1879.) Ich citire im folgenden die erste Abhandlung kurz durch B., die zweite durch D.

allgemeine Theorie der Körper im Sinne der Dedekind'schen Auffassungen weiter auszuführen, als dies von Herrn Dedekind selbst geschehen ist. Dies bildet den Gegenstand des ersten Theiles dieser Arbeit; einige gelegentliche Andeutungen des Herrn Dedekind in seinen Schriften habe ich dabei nach bestem Können verwerthet.

Auf das hier behandelte Problem bezieht sich auch — mehr oder weniger direct — die grosse Reihe glänzender Untersuchungen, welche Herr Kronecker über Algebra und Arithmetik veröffentlicht und in den Grundzügen einer arithmetischen Theorie der algebraischen Grössen*) zusammengefasst hat. Bei der grossen Verschiedenheit zwischen den Kronecker'schen und den Dedekind'schen Methoden war es mir bislang nicht möglich, den inneren Zusammenhang, der nothwendig in letzter Instanz zwischen diesen verschiedenen Behandlungsweisen desselben Gegenstandes bestehen muss, zu erkennen. Diese Lücke, die ich selbst sehr lebhaft bedauere, hoffe ich in Zukunft ausfüllen zu können; für jetzt haben mir im Wesentlichen nur die Dedekind'schen Arbeiten als Grundlage gedient.

*) Festschrift zu Herrn Kummers 50jährigem Doctor-Jubiläum. Berlin 1882. Auch in Crelles Journ. Bd. 92 erschienen.

I.

Endliche Körper.

1. Ein System von Zahlen, welches die charakteristische Eigenschaft besitzt, dass die Summe, die Differenz, das Product und der Quotient irgend zweier Zahlen des Systems sich wieder in dem Systeme vorfindet, heisst nach Herrn Dedekind ein Körper von Zahlen. Von den hier genannten Rechenoperationen hat allein die Division durch Null als unzulässig zu gelten, weil sie ein unbestimmtes Resultat liefert. Der Definition zufolge würde die Zahl Null für sich allein einen Zahlkörper bilden, doch wird dieser Fall füglich von der Betrachtung ganz ausgeschlossen. Dann findet sich in jedem Körper eine von Null verschiedene Zahl und folglich auch die Eins als Quotient zweier gleichen Zahlen und jede rationale Zahl, weil sie durch rationale Operationen aus der Eins erhalten werden kann. Da aber die rationalen Zahlen für sich allein offenbar auch einen Körper bilden, so können wir sagen, indem wir einen Körper dann Theiler eines andern Körpers nennen, wenn jede Zahl des ersten auch dem zweiten angehört: Der Körper der rationalen Zahlen ist ein Theiler jedes Zahlkörpers. Der Körper der rationalen Zahlen ist also der niedrigste, wie der Körper aller überhaupt möglichen Zahlen der höchste aller Zahlkörper ist. Sind zwei Körper durch einander theilbar, so sind sie identisch.

Den hier eingeführten Begriff der Theilbarkeit der Körper verwenden wir sogleich zur Definition des grössten gemein-

schaftlichen Theilers und des kleinsten gemeinschaftlichen Multiplums zweier Körper. Das System derjenigen Zahlen, welche zwei Körpern A und B gemeinschaftlich angehören, bildet offenbar wieder einen Zahlkörper; denn sind μ und μ' zwei Zahlen, welche beiden Körpern A und B angehören und bezeichnen wir mit dem Zeichen o irgend eine der vier rationalen Rechenoperationen, so gehört auch die Zahl $\mu o \mu'$ beiden Körpern gemeinsam an. Dieser Körper Δ der den beiden Körpern gemeinschaftlichen Zahlen ist ein Theiler beider Körper; er heisst der grösste gemeinschaftliche Theiler, weil er ein Multiplum jedes gemeinschaftlichen Theilers beider Körper ist. Ist der grösste gemeinschaftliche Theiler zweier Körper der Körper R der rationalen Zahlen, so heissen die Körper relativ prim oder ohne gemeinschaftlichen Theiler. Bilden wir andererseits das System aller derjenigen Zahlen, welche durch rationale Operationen aus Zahlen des Körpers A und Zahlen des Körpers B gebildet werden können, so erhalten wir einen Körper M, welcher ein Multiplum beider Körper ist und das kleinste gemeinschaftliche Multiplum heisst, weil er ein Divisor jedes gemeinschaftlichen Multiplums beider Körper ist. Man kann jede Zahl des Körpers M durch das Symbol $\Sigma\alpha\beta$ bezeichnen; denn um alle Zahlen von M zu erhalten, reicht es offenbar aus, zuerst alle Producte irgend einer Zahl α des Körpers A und irgend einer Zahl β des Körpers B zu bilden und sodann diese Producte auf alle möglichen Arten zu summiren. Ist A ein Multiplum von B, so ist das kleinste gemeinschaftliche Vielfache der Körper A, der grösste gemeinschaftliche Theiler der Körper B. Die Ausdehnung der beiden Begriffe auf mehr als zwei Körper bedarf keiner Erläuterung.

2. Um nun zur Definition der endlichen Körper zu gelangen, führen wir den Begriff des unabhängigen Systems ein. Ein System von n Zahlen $\omega_1, \omega_2, \ldots \omega_n$ bildet in Beziehung auf einen Körper A ein reductibeles oder irreductibeles System (abhängiges oder unabhängiges System), je nachdem die Gleichung

$$\Sigma_i \alpha_i \omega_i = 0 \qquad i = 1, \ldots n.$$

durch n Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$, welche dem Körper A angehören und nicht sämmtlich verschwinden, gelöst werden kann oder nicht. (D. S. 465, Anm.) Diese Definition hat der Regel nach nur dann Interesse, wenn die Zahlen $\omega_1, \omega_2, \ldots \omega_n$ dem Körper A nicht angehören; denn irgend zwei Zahlen von A sind in Beziehung auf A abhängig. Eine Zahl bildet dann und nur dann in Beziehung auf A ein abhängiges System, wenn sie Null ist. Ist der Körper A, zu welchem das System der Zahlen $\omega_1, \omega_2, \ldots \omega_n$ in Beziehung gesetzt wird, der Körper R der rationalen Zahlen, so spricht man schlechthin von einem abhängigen oder unabhängigen Systeme ohne weiteren Zusatz.

Es gilt nun der wichtige Satz: Sind die n Zahlen $\omega_1, \omega_2, \ldots \omega_n$ in Beziehung auf den Körper A unabhängig, so bilden in Beziehung auf denselben Körper die n Zahlen

$$\omega_k' = \Sigma_i \alpha_i^{(k)} \omega_i \qquad \overset{i}{k} = 1, 2, \ldots n,$$

welche durch Composition mit den n^2 dem Körper A angehörigen Zahlen $\alpha_i^{(k)}$ aus den ω gebildet sind, ein abhängiges oder unabhängiges System, je nachdem die Determinante

$$\alpha = \Sigma \pm \alpha_1' \alpha_2'' \ldots \alpha_n^{(n)}$$

verschwindet oder von Null verschieden ist.

Denn sollen $\omega_1', \omega_2' \ldots \omega_n'$ in Beziehung auf A abhängig sein, so muss die Summe

$$\Sigma_k \xi_k \omega_k' = \Sigma_{ki} \xi_k \alpha_i^{(k)} \omega_i$$

für n Zahlen $\xi_1, \xi_2, \ldots \xi_n$, welche sich in A finden und nicht alle Null sind, zum Verschwinden gebracht werden können. Da aber $\omega_1, \omega_2, \ldots \omega_n$ unabhängig sind, so müssen die n Gleichungen

$$\Sigma_k \alpha_i^{(k)} \xi_k = 0$$

durch nicht verschwindende Werthe von ξ befriedigt werden, und dazu ist $\alpha = 0$ nothwendig. Ist umgekehrt $\alpha = 0$, so weist man durch eine bekannte Methode, welche der Theorie der linearen Gleichungen angehört, leicht nach, dass die Zahlen $\omega_1', \omega_2', \ldots \omega_n'$ ein abhängiges System bilden. Man hat zu diesem Zwecke in dem quadratischen Systeme der Coeffi-

cienten $a_i^{(k)}$ eine Unterdeterminante m^{ten} Grades zu ermitteln, welche nicht verschwindet, während alle Minoren höheren Grades verschwinden; gehört dieselbe, was man ohne Beschränkung der Allgemeinheit annehmen darf, zu den Zahlen $\omega_1', \omega_2', \ldots \omega_m'$ $(m < n)$, so bilden $\omega_1', \omega_2', \ldots \omega_m'$ in Beziehung auf A ein unabhängiges System, während sie mit irgend einer der noch übrigen Zahlen ω' ein abhängiges System bilden.

3. Ein Körper heisst nun ein endlicher Körper n^{ten} Grades, wenn es in ihm n von einander unabhängige Zahlen giebt, während irgend $(n + 1)$ Zahlen von einander abhängig sind. Ein solches unabhängiges System von n Zahlen, welches mit irgend einer weiteren Zahl des Körpers ein abhängiges System bildet, heisst eine Basis des Körpers. Ist Ω ein Körper n^{ten} Grades und $\omega_1, \omega_2, \ldots \omega_n$ eine Basis, so bilden die n mit den n^2 rationalen Zahlen $r_i^{(k)}$ gebildeten Zahlen:

$$(1) \quad \omega_k' = \Sigma_i r_i^{(k)} \omega_i, \qquad i, k = 1, 2, \ldots n$$

die dem Körper auch angehören, ebenfalls eine Basis, wenn die Determinante

$$r = \Sigma \pm r_1' r_2'' \ldots r_n^{(n)}$$

von Null verschieden ist (§ 2). Sind umgekehrt $\omega_1, \omega_2, \ldots \omega_n$ und $\omega_1', \omega_2', \ldots \omega_n'$ zwei Basen des Körpers Ω, so bestehen n Gleichungen (1) und die Determinante r derselben ist von Null verschieden, so dass die Gleichungen umkehrbar sind. Dieser Satz kann, wie man leicht erkennt, auch dahin ausgesprochen werden: Jeder Körper n^{ten} Grades hat nur einen Theiler n^{ten} Grades, nämlich sich selbst.

Jede Zahl ω des Körpers Ω bildet mit den Basiszahlen $\omega_1, \omega_2, \ldots \omega_n$ zusammen ein abhängiges System; d. h. es besteht eine Gleichung

$$r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n + r\omega = 0,$$

in welcher die Zahlen $r_1, r_2, \ldots r_n, r$ rationale, nicht sämmtlich verschwindende Zahlen bedeuten, deren letzte r wegen der Unabhängigkeit von $\omega_1, \omega_2, \ldots \omega_n$ nicht Null sein kann. Hieraus folgt, dass jede Zahl ω des Körpers in die Form gesetzt werden kann

$$\omega = \Sigma_i x_i \omega_i \qquad i = 1, \ldots n$$

worin die x rationale, beliebige Zahlen bedeuten. Umgekehrt gehört zu jedem Werthsysteme rationaler $x_1, x_2, \ldots x_n$, eine dem Körper Ω angehörige Zahl $\Sigma_i x_i \omega_i$, und zu zwei verschiedenen Werthsystemen x gehören auch zwei verschiedene Zahlen ω wegen der Irreductibilität der Basis.

4. Besitzt der Körper Ω vom n^{ten} Grade einen Divisor A vom m^{ten} Grade, dessen Basis durch die Zahlen

$$(1) \quad \alpha_1, \alpha_2, \ldots \alpha_m$$

gebildet wird, so giebt es entweder ausser den Zahlen $\Sigma_i x_i \alpha_i$ ($i = 1, \ldots m$) keine Zahl in Ω, — dann ist Multiplum und Divisor identisch und $n = m$ (§ 3) — oder es giebt in Ω eine Zahl ω', welche nicht in A vorkommt; dann bilden wir die Zahlen

$$(2) \quad \omega'\alpha_1, \omega'\alpha_2, \ldots \omega'\alpha_m.$$

Die Zahlen der zweiten Reihe bilden offenbar auch ein unabhängiges System; sie bilden aber sogar mit den Zahlen der ersten Reihe zusammen ein solches. Wäre nämlich

$$x_1\alpha_1 + x_2\alpha_2 + \ldots + x_m\alpha_m + y_1\omega'\alpha_1 + y_2\omega'\alpha_2 + \ldots + y_m\omega'\alpha_m = 0,$$

so wäre die Zahl

$$-\omega' = \frac{\Sigma_i x_i \alpha_i}{\Sigma_i y_i \alpha_i}, \qquad i = 1, \ldots m,$$

deren Nenner nicht verschwindet, gegen die Voraussetzung eine Zahl des durch die Reihe (1) definirten Körpers. Entweder ist nun $n = 2m$, dann bilden die Reihen (1) und (2) zusammen eine Basis von Ω, oder es ist $n > 2m$, dann giebt es in Ω eine Zahl ω'', welche mit den Zahlen der Reihen (1) und (2) zusammen ein unabhängiges System bildet. Dann bilden wir die dritte Reihe

$$(3) \quad \omega''\alpha_1, \omega''\alpha_2, \ldots \omega''\alpha_m$$

und weisen nach, dass die drei Reihen (1), (2), (3) ein unabhängiges System bilden. Wäre nämlich

$$\Sigma_i x_i \alpha_i + \omega' \Sigma_i y_i \alpha_i + \omega'' \Sigma_i z_i \alpha_i = 0,$$

so könnte $\Sigma_i z_i \alpha_i$ nicht verschwinden und folglich wäre

$$-\omega'' = \frac{\Sigma_i x_i \alpha_i}{\Sigma_i z_i \alpha_i} + \omega' \frac{\Sigma_i y_i \alpha_i}{\Sigma_i z_i \alpha_i}$$

eine Zahl, welche linear aus den Zahlen der Reihen (1) und (2) mit rationalen Coefficienten zusammensetzbar ist, was der Annahme

widerspricht. Setzt man dieses Exhaustionsverfahren fort, so erkennt man, dass dasselbe einmal abbrechen muss und dass in jedem Falle n ein Multiplum von m sein muss. Also haben wir den Satz, wenn wir der Kürze halber mit

$$\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$$

denjenigen Körper bezeichnen, welcher die Zahlen $\alpha_1, \alpha_2, \ldots \alpha_m$ zu Basiszahlen hat:

Ist Ω ein Körper n^{ten} Grades und $\{\alpha_1, \alpha_2, \ldots \alpha_m\} = A$ ein Theiler desselben vom m^{ten} Grade, so ist n ein Multiplum von m, $n = mp$, und man kann als Basis von Ω wählen die Zahlen:

$$(T) \quad \begin{cases} \alpha_1, \alpha_2, \ldots \alpha_m; \\ \omega'\alpha_1, \omega'\alpha_2, \ldots, \omega'\alpha_m; \\ \omega''\alpha_1, \omega''\alpha_2, \ldots \omega''\alpha_m; \\ \ldots\ldots\ldots\ldots\ldots \\ \omega^{(p-1)}\alpha_1, \omega^{(p-1)}\alpha_2, \ldots, \omega^{(p-1)}\alpha_m. \end{cases}$$

Hierin bedeutet ω' eine Zahl, welche nicht dem Körper $\{\alpha_1, \alpha_2, \ldots \alpha_m\}$ angehört, ω'' eine Zahl, welche nicht linear aus den Zahlen $\alpha_1, \alpha_2, \ldots \alpha_m, \omega'\alpha_1, \ldots \omega'\alpha_m$ mit rationalen Coefficienten componirbar ist u. s. w. Der letzte Satz kann auch dahin ausgesprochen werden, dass die p Zahlen $1, \omega', \omega'', \ldots \omega^{(p-1)}$ in Beziehung auf den Körper A ein unabhängiges System bilden, während offenbar irgend $p+1$ Zahlen des Tableaus (T) und folglich auch irgend $p+1$ Zahlen des Körpers Ω in Beziehung auf A ein abhängiges System bilden. Diese Bemerkung veranlasst uns, die Begriffe der Basis und des Grades eines endlichen Körpers zu erweitern, so dass die neuen Begriffe sich ganz so zu den alten verhalten, wie sich der Begriff des in Beziehung auf einen Körper A abhängigen Systems zu dem Begriffe des schlechthin abhängigen Systems verhält. Ein Körper Ω heisse nämlich in Beziehung auf einen Divisor A vom p^{ten} Grade, wenn es in ihm p in Beziehung auf A unabhängige Zahlen giebt, während irgend $p+1$ Zahlen in Beziehung auf A abhängig sind, und ein System von p solchen in Beziehung auf A unabhängigen Zahlen heisse eine Basis von Ω in Beziehung auf A. Die alten Begriffe gehen wieder aus

den neuen erweiterten hervor, indem man annimmt, dass der Theiler A, zu dem Ω in Beziehung gesetzt wird, der Körper R der rationalen Zahlen ist, und der vorige Satz erhält die kurze Fassung:

Ein Körper Ω vom Grade n hat in Beziehung auf einen Divisor A vom Grade m den Grad $p = \frac{n}{m}$.

5. Jede Zahl Θ eines endlichen Körpers ist eine algebraische Zahl, d. h. sie genügt einer Gleichung von endlichem Grade mit rationalen Coefficienten. Denn hat der Körper den Grad n, so sind die n + 1 Zahlen

$$1, \Theta, \Theta^2, \ldots . \Theta^n,$$

welche auch dem Körper angehören, von einander abhängig; d. h. es giebt (n + 1) rationale Zahlen

$$x_0, x_1, x_2, \ldots . x_n,$$

die nicht alle verschwinden, so dass

$$x_0 + x_1\Theta + x_2\Theta^2 + \ldots + x_n\Theta^n = 0 \text{ ist.}$$

Dass diese Gleichung aber im Körper R der rationalen Zahlen irreductibel ist, ist ohne weiteres natürlich nicht nothwendig. Genügt aber die Zahl Θ der irreductibelen Gleichung n^{ten} Grades

$$f(\Theta) \equiv \Theta^n + a_1\Theta^{n-1} + a_2\Theta^{n-2} + \ldots + a_n = 0$$

mit rationalen Coefficienten, so bilden alle Zahlen, welche durch rationale Operationen aus Θ gebildet sind, einen Körper, und dieser Körper ist n^{ten} Grades, weil sich jede solche Zahl stets und nur auf eine Weise als ganze rationale Function niedrigeren als n^{ten} Grades von Θ darstellen lässt. Denn ist g(x) eine ganze Function n^{ten} oder höheren Grades, so bestimme man den Rest r(x), welcher sich bei der Division von g(x) durch f(x) einstellt; dieser ist von niedrigerem als dem n^{ten} Grade und es ist $g(\Theta) = r(\Theta)$; ist aber $\frac{g(x)}{h(x)}$ eine gebrochene Function von x, so muss h(x) jedenfalls prim zu f(x) sein, weil sonst der Nenner $h(\Theta)$ gleich Null wäre; folglich kann man durch die Methode des grössten gemeinschaftlichen Theilers zwei ganze Functionen h'(x) und f'(x) bestimmen, so dass

$$g(x) = h(x)h'(x) + f(x)f'(x)$$

ist, und folglich ist

$$\frac{g(\Theta)}{h(\Theta)} = h'(\Theta)$$

also als ganze Function von Θ dargestellt.

Eine solche Zahl Θ, welche durch ihre n ersten Potenzen (von Θ^0 bis Θ^{n-1}) einen Körper erzeugt, welcher vom n^{ten} Grade ist, wollen wir eine constituirende Zahl eines Körpers nennen. Haben wir aber einen beliebigen Körper Ω n^{ten} Grades, so wissen wir bis jetzt bloss, dass jede seiner Zahlen einen Körper constituirt, welcher ein (echter oder unechter) Theiler von Ω ist, und dessen Grad also nach § 4 ein Theiler von n sein muss. Dass aber in jedem Körper n^{ten} Grades auch Zahlen existiren, welche einer irreductibelen Gleichung n^{ten} Grades genügen und also constituirende Zahlen sind, bedarf eines besonderen Beweises. Nachdem derselbe geführt ist, wird es sich zeigen, dass der zuletzt besprochene Fall eines Zahlkörpers den allgemeinen anfangs eingeführten Begriff vollständig zu ersetzen im Stande ist. Zu diesem Zwecke beweisen wir einen Satz, welcher uns auch anderweitig von Nutzen sein wird.*)

6. Es mögen die algebraischen Zahlen β und α den zwei im Körper der rationalen Zahlen irreductibelen Gleichungen resp. vom m^{ten} und n^{ten} Grade genügen:

$$(B)\quad g(\beta) \equiv \beta^m + b_1\beta^{m-1} + \ldots + b_{m-1}\beta + b_m = 0$$

$$(A)\quad h(\alpha) \equiv \alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0;$$

so constituiren die beiden Zahlen zwei Körper B und A vom m^{ten} und n^{ten} Grade. Dann ist es möglich, dass die zweite Gleichung (A) im Körper B reductibel wird; in jedem Falle sei

$$(A')\quad F(x, \beta) \equiv x^{n'} + \beta_1 x^{n'-1} + \ldots + \beta_{n'-1} x + \beta_{n'}$$

diejenige mit Zahlen des Körpers B gebildete, im Körper B irreductibele Function, welche durch $x = \alpha$ annullirt wird. Ihr Grad n' ist $\leq n$ und im Falle $n' = n$ ist $F(x, \beta) \equiv h(x)$. Dann sind also

$$\alpha^0, \alpha^1, \alpha^2, \ldots \alpha^{n'-1}$$

*) Vergl. Dirichlet, Zahlentheorie, zweite Auflage, S. 427, Anm.

in Beziehung auf B unabhängig, während sie mit $\alpha^{n'}$ zusammen ein in Beziehung auf B abhängiges System bilden, und die Basis des kleinsten gemeinschaftlichen Multiplums M der beiden Körper A und B wird also nach § 4 durch die mn' Zahlen gebildet:

$$(M)\quad \begin{cases} 1,\ \beta,\ \ldots\ \beta^{m-1}; \\ \alpha,\ \alpha\beta,\ \ldots\ \alpha\beta^{m-1}; \\ \ldots\ldots\ldots\ldots \\ \alpha^{n'-1},\ \alpha^{n'-1}\beta,\ \ldots,\ \alpha^{n'-1}\beta^{m-1}. \end{cases}$$

Wir behaupten, dass die rationale Zahl s so bestimmt werden könne, dass die Zahl $\beta + s\alpha$ constituirende Zahl des Körpers M wird; oder, was auf dasselbe hinauskommt, es kann $\beta + s\alpha$ für unbestimmt gelassenes (rationales) s nicht einer Gleichung mit rationalen Coefficienten genügen, deren Grad kleiner als mn' wäre.

Bildet man der Reihe nach die Potenzen

$$(\beta + s\alpha)^0,\ (\beta + s\alpha)^1,\ (\beta + s\alpha)^2,\ \ldots.$$

und stellt dieselben mit Hilfe der Gleichungen (B) und (A') als lineare Functionen der Grössen (M) dar, deren Coefficienten ganze Functionen von s mit rationalen Coefficienten sind, so ist klar, dass man die Grössen (M) aus den p ersten dieser Gleichungen eliminiren kann, wobei p eine Zahl bedeutet, die jedenfalls nicht grösser als mn' sein kann. Es genügt also $\beta + s\alpha$ einer Gleichung p^{ten} Grades

$$(C)\quad f(x, s) \equiv C_0x^p + C_1x^{p-1} + \ldots. + C_{p-1}x + C_p = 0,$$

deren Coefficienten ganze Functionen von s mit rationalen Coefficienten sind. Es ist zu beweisen, dass p auch nicht kleiner als mn' sein kann.

Die Gleichung (C) wird, wenn man $x = \beta + s\alpha$ setzt, auf Grund der Gleichungen (B) und (A') zu einer in Beziehung auf die Variabele s identischen Gleichung. Entwickelt man nun die Function f(x, s) nach s, so erhält man die endliche Reihe:

$$(1)\quad f(x, s) = f(x, 0) + \frac{f_s'(x, 0)}{1!}s + \frac{f_{ss}''(x, 0)}{2!}s^2 + \ldots.$$

und hierin sind die Functionen $f(x, 0)$, $f_s'(x, 0)$, $f_{ss}''(x, 0)$ ganze Functionen von x mit rationalen Coefficienten, nämlich

$$(2)\begin{cases} f(x,0) = (C_0)_0 x^p + (C_1)_0 x^{p-1} + \ldots + (C_{p-1})_0 x + (C_p)_0 \\ f_s'(x,0) = \left(\frac{dC_0}{ds}\right)_0 x^p + \left(\frac{dC_1}{ds}\right)_0 x^{p-1} + \ldots + \left(\frac{dC_{p-1}}{ds}\right)_0 x + \left(\frac{dC_p}{ds}\right)_0 \\ f_{ss}''(x,0) = \left(\frac{d_2C_0}{ds^2}\right)_0 x^p + \left(\frac{d_2C_1}{ds^2}\right)_0 x^{p-1} + \ldots + \left(\frac{d^2C_{p-1}}{ds^2}\right)_0 x + \left(\frac{d^2C_p}{ds^2}\right)_0 \\ \ldots\ldots \end{cases}$$

Setzt man in diesen Functionen $x = \beta + s\alpha$ und entwickelt nach Potenzen von s, so erhält man:

$$(3)\begin{cases} f(\beta + s\alpha, 0) = f(\beta, 0) + f_x'(\beta, 0)\,\frac{s\alpha}{1!} + f_{xx}''(\beta, 0)\,\frac{s^2\alpha^2}{2!} + \\ \qquad \ldots + f_{x^{(p)}}^{(p)}(\beta, 0)\,\frac{s^p\alpha^p}{p!} \\ f_s'(\beta + s\alpha, 0) = f_s'(\beta, 0) + f_{sx}''(\beta, 0)\,\frac{s\alpha}{1!} + f_{sxx}'''(\beta, 0)\,\frac{s^2\alpha^2}{2!} \\ \qquad + \ldots + f_{sx^{(p)}}^{(p+1)}(\beta, 0)\,\frac{s^p\alpha^p}{p!} \\ f_s''(\beta + s\alpha, 0) = f_{ss}''(\beta, 0) + f_{ssx}'''(\beta, 0)\,\frac{s\alpha}{1!} + f_{ssxx}^{(4)}(\beta, 0)\,\frac{s^2\alpha^2}{2!} \\ \qquad + \ldots + f_{ssx^{(p)}}^{(p+2)}(\beta, 0)\,\frac{s^p\alpha^p}{p!} \\ \ldots\ldots\ldots \end{cases}$$

Hierin bedeutet $f_{s^{(m)}x^{(n)}}^{(m+n)}$ die $(m+n)^{te}$ Derivirte von $f(x, s)$, welche man erhält, wenn man m mal nach s und n mal nach x differentiirt; also:

$$(4)\begin{cases} f(\beta, 0) = (C_0)_0\,\beta^p + (C_1)_0\,\beta^{p-1} + \ldots + (C_{p-1})_0\beta + (C_p)_0 \\ f_x'(\beta,0) = p(C_0)_0\beta^{p-1} + (p-1)\,(C_1)_0\,\beta^{p-2} + \ldots + (C_{p-1})_0 \\ f_{xx}''(\beta, 0) = p\,.\,(p-1)\,(C_0)_0\,\beta^{p-2} + (p-1)\,.\,(p-2)\,(C_1)_0\,\beta^{p-3} \\ \qquad + \ldots + 2\,(C_{p-2})_0 \\ \ldots\ldots\ldots\ldots \\ f_s'(\beta, 0) = \left(\frac{dC_0}{ds}\right)_0\beta^p + \left(\frac{dC_1}{ds}\right)_0\beta^{p-1} + \ldots + \left(\frac{dC_{p-1}}{ds}\right)_0\beta + \left(\frac{dC_p}{ds}\right)_0 \\ f_{sx}''(\beta,0) = p\left(\frac{dC_0}{ds}\right)_0\beta^{p-1} + (p-1)\left(\frac{dC_1}{ds}\right)_0\beta^{p-2} + \ldots + \left(\frac{dC_{p-1}}{ds}\right)_0 \\ f_{sxx}'''(\beta,0) = p(p-1)\left(\frac{dC_0}{ds}\right)_0\beta^{p-2} + (p-1)(p-2)\left(\frac{dC_1}{ds}\right)_0\beta^{p-3} \\ \qquad + \ldots + 2\left(\frac{dC_{p-2}}{ds}\right)_0 \\ \ldots\ldots\ldots \end{cases}$$

$$
\begin{cases}
f''_{ss}(\beta,0) = \left(\frac{d^2C_0}{ds^2}\right)_0 \beta^p + \left(\frac{d^2C_1}{ds^2}\right)_0 \beta^{p-1} + \ldots + \left(\frac{d^2C_{p-1}}{ds^2}\right)_0 \beta \\
\qquad\qquad + \left(\frac{d^2C_p}{ds^2}\right)_0 \\
f'''_{ssx}(\beta,0) = p \cdot \left(\frac{d^2C_0}{ds^2}\right)_0 \beta^{p-1} + (p-1)\left(\frac{d^2C_1}{ds^2}\right)_0 \beta^{p-2} + \ldots \\
\qquad\qquad + \left(\frac{d^2C_{p-1}}{ds^2}\right)_0 \\
f^{(4)}_{ssxx}(\beta,0) = p \cdot (p-1)\left(\frac{d^2C_0}{ds^2}\right)_0 \beta^{p-2} + (p-1)(p-2)\left(\frac{d^2C_1}{ds^2}\right)_0 \beta^{p-3} \\
\qquad\qquad + \ldots + 2\left(\frac{d^2C_{p-2}}{ds^2}\right)_0 \\
\ldots\ldots
\end{cases}
$$

Setzt man nun die Entwickelungen (3) in (1) ein, so erhält man: es muss identisch in Beziehung auf s Null sein:

$$f(\beta+s\alpha,s) \text{ d. i.}$$

$$
\begin{aligned}
&\left[f(\beta,0) + f'_x(\beta,0)\frac{s\alpha}{1!} + f''_{xx}(\beta,0)\frac{s^2\alpha^2}{2!} + \ldots + f^{(p)}_{x^{(p)}}(\beta,0)\frac{s^p\alpha^p}{p!}\right] \\
&+\left[f'_s(\beta,0) + f''_{sx}(\beta,0)\frac{s\alpha}{1!} + f'''_{sxx}(\beta,0)\frac{s^2\alpha^2}{2!} + \ldots \right. \\
&\qquad \left. + f^{(p+1)}_{sx^{(p)}}(\beta,0)\frac{s^p x^p}{p!}\right]\frac{s}{1!} \\
&+\left[f''_{ss}(\beta,0) + f'''_{ssx}(\beta,0)\frac{s\alpha}{1!} + f^{(4)}_{ssxx}(\beta,0)\frac{s^2\alpha^2}{2!} + \ldots \right. \\
&\qquad \left. + f^{(p+2)}_{ssx^{(p)}}(\beta,0)\frac{s^p\alpha^p}{p!}\right]\frac{s^2}{2!} + \ldots .
\end{aligned}
$$

oder wenn man nach Potenzen von s ordnet:

$$
(5)\quad
\begin{cases}
f(\beta,0) + \frac{s}{1!}(\alpha f'_x(\beta,0) + f'_x(\beta,0)) \\
\quad + \frac{s^2}{2!}(\alpha^2 f''_{xx}(\beta,0) + 2\alpha f''_{sx}(\beta,0) + f''_{ss}(\beta,0)) \\
+ \frac{s^3}{3!}(\alpha^3 f'''_{xxx}(\beta,0) + \binom{3}{1}\alpha^2 f'''_{sxx}(\beta,0) + \binom{3}{2}\alpha f'''_{ssx}(\beta,0) \\
\qquad + f'''_{sss}(\beta,0)) \\
+ \ldots .
\end{cases}
$$

$$\left| + \frac{s^{n'-1}}{(n'-1)!} (\alpha^{n'-1} f^{(n'-1)}_{x(n'-1)}(\beta,0) + \binom{n'-1}{1} \alpha^{n'-2} f^{(n'-1)}_{sx\,(n'-2)}(\beta,0) + \ldots) \right.$$
$$\left. + \ldots \right.$$

Wir hätten diese Gleichung etwas schneller auf Grund des Taylorschen Satzes für mehrere Variabelen ableiten können; doch ist der Durchgang durch die Gleichung (1) für uns nicht überflüssig. Weil aber der Ausdruck (5) identisch in Beziehung auf s verschwindet und weil α im Zahlkörper B keiner Gleichung genügen kann, deren Grad niedriger als n' wäre, so schliessen wir:

$$(6) \quad \begin{cases} f(\beta,0) = 0 \\ f'_x(\beta,0) = 0, \quad f'_s(\beta,0) = 0 \\ f''_{xx}(\beta,0) = 0, \quad f''_{sx}(\beta,0) = 0, \quad f''_{ss}(\beta,0) = 0 \\ f^{(n'-1)}_{x(n'-1)}(\beta,0) = 0 \quad f^{(n'-1)}_{sx(n'-2)}(\beta,0) = 0 \quad \ldots \quad f^{(n'-1)}_{s(n'-1)}(\beta,0) = 0; \end{cases}$$

d. h. es müssen für das Werthsystem $x = \beta$, $s = 0$ alle Differentiale der Function f(x, s) bis zum $(n'-1)^{ten}$ verschwinden. Betrachten wir nunmehr die Function p^{ten} Grades von x f(x, 0), so lehrt die erste von den Gleichungen des Systemes (6) zunächst, dass sie für $x = \beta$ verschwindet und folglich wegen der Irreductibilität von g(x) durch g(x) theilbar ist. Es ist aber f(x) sogar durch die n'^{te} Potenz von g(x) theilbar, wie aus den ersten Gleichungen der folgenden Zeilen hervorgeht; denn setzt man

$$f(x, 0) = g(x)\ v(x),$$

so lehrt die Differentiation nach x,

$$f'_x(x, 0) = g(x)\ v'(x) + g'(x)\ v(x),$$

da $g'(\beta)$ nicht verschwinden kann, dass $v(\beta)$ verschwinden und folglich v(x) durch g(x) theilbar sein muss; und indem man dieses Verfahren solange fortsetzt, bis auch die Gleichung $f^{(n'-1)}_{x(n'-1)}(\beta, 0) = 0$ Verwendung gefunden und sich die n'^{te} Potenz von g(x) aus f(x, o) herausgehoben hat, findet man:

$$(7) \quad f(x, 0) = g(x)^{n'}\ h(x)$$

und ebenso für die anderen Functionen $f'_s(x, 0)$, $f''_{ss}(x, 0)$, $\ldots$ $f^{(n'-1)}_{s(n'-1)}(x, 0)$:

$$(8)\quad \begin{cases} f_s'(x,0) = g(x)^{n'-1}\, h'(x) \\ f_{ss}''(x,0) = g(x)^{n'-2}\, h''(x) \\ \cdots\cdots \\ f_{s^{(n'-1)}}^{(n'-1)}(x,0) = g(x)\; h^{(n'-1)}(x); \end{cases}$$

Wenn man diese Gleichungen in (1) einsetzt, so findet man die Entwickelung:

$$(9)\quad f(x,s) = g(x)^{n'}\, h(x) + g(x)^{n'-1}\, h'(x)\, s + g(x)^{n'-2}\, h''(x)\,.\, s^2 + \ldots,$$

und hieraus folgt nunmehr, da g(x) vom Grade m ist, dass das erste Glied der Entwickelung rechts und folglich auch f(x, s) mindestens vom Grade mn' sein muss. Da übrigens der Grad von f(x, s), so lange diese Function irreductibel ist, auch nicht kleiner sein kann, so muss h(x) eine Constante sein. Wir haben also jetzt den wichtigen Satz, wenn wir an die Stelle der nicht homogenen Verbindung $\beta + sa$ die homogene Form $a\alpha + b\beta$ setzen:

Wenn die algebraische Zahl α den Körper A, die algebraische Zahl β den Körper B constituirt, so kann man stets zwei rationale Zahlen a und b so bestimmen, dass die Zahl $a\alpha + b\beta$ das kleinste gemeinschaftliche Multiplum M der beiden Körper A und B constituirt.

7. Aus dem gewonnenen Satze ziehen wir einige Folgerungen, deren wesentlichste die Constitution eines beliebigen endlichen Körpers durch eine in ihm enthaltene Zahl betrifft.

1. Ist Ω irgend ein Körper n^{ten} Grades und α eine in ihm enthaltene Zahl, so constituirt α einen Körper A, welcher jedenfalls ein (echter oder unechter) Theiler von Ω ist und dessen Grad also nach § 4 ein Theiler von n sein muss. Ist der Grad von A gleich n, so ist $A = \Omega$ und α constituirende Zahl des Körpers; ist aber der Grad kleiner als n, so giebt es in Ω eine Zahl β, welche nicht in A enthalten ist und einen Körper B constituirt. Das kleinste gemeinschaftliche Multiplum M der beiden Körper A und B hat einen höheren Grad als A, weil sonst B in A enthalten wäre, und kann nach dem vorherigen Satze durch eine Zahl $a\alpha + b\beta$ constituirt werden. Ist der Grad von M gleich n, so ist $M = \Omega$ und $a\alpha + b\beta$ constituirende Zahl; anderenfalls

hat man wieder weiter zu gehen und muss, weil n endlich und jeder folgende Divisor immer von höherem Grade als der vorhergehende ist, nothwendigerweise nach einer endlichen Anzahl von Malen zu einem Abschlusse gelangen. Also der Satz:

In einem Körper n^{ten} Grades giebt es stets unendlich viele Zahlen, welche einer irreductibelen Gleichung n^{ten} Grades genügen und deren n erste Potenzen als Basis des Körpers gewählt werden können.

Alle solche constituirenden Zahlen eines Körpers Ω bilden dasjenige, was Herr Kronecker eine Gattung algebraischer Zahlen nennt, während ein Zahlkörper nach Kronecker'scher Terminologie ein Gattungsbereich ist.*) Von zwei constituirenden Zahlen kann jede als ganze rationale Function $(n-1)^{ten}$ Grades mit rationalen Coefficienten der anderen dargestellt werden.

2. Der am Ende des vorigen Paragraphen angegebene Satz lässt sich ohne weiteres auf mehr als zwei Körper ausdehnen. Wir können jetzt auf Grund des soeben Bewiesenen sagen:

Hat man mehrere Körper $A, B, \Gamma \ldots$ und sind resp. $\alpha, \beta, \gamma \ldots$ constituirende Zahlen dieser Körper, so kann man ebenso viele rationale Zahlen a, b, c ... so wählen, dass

$$a\alpha + b\beta + c\gamma + \ldots$$

constituirende Zahl des kleinsten gemeinschaftlichen Multiplums M der Körper $A, B, \Gamma \ldots$ wird.

3. Schliesslich lassen sich aus dem Gange des Beweises des Satzes in § 6 einige Folgerungen ziehen, die von Interesse sind. Der Körper M ist, wie wir gesehen, vom Grade $p = mn'$; er ist aber ein Multiplum nicht bloss von B, sondern auch von A; und folglich ist (nach § 4) mn' ein Multiplum vom n:

$$(10) \quad mn' = m'n \text{ oder } m : n = m' : n'.$$

*) Grundzüge § 3, Monatsberichte d. Berl. Akad. März 1879, II, § 1; doch beziehen sich die Kronecker'schen Begriffe nicht bloss auf „Zahlen", sondern auch auf „Functionen".

Die ganze Zahl m', die sich hier einstellt, hat aber auch eine charakteristische Bedeutung. Der Beweis rechnete nämlich mit der Möglichkeit, dass die im Körper der rationalen Zahlen irreductibele Gleichung n^{ten} Grades (A) im Körper $\boldsymbol{B}$ reductibel und auf den n'^{ten} Grad erniedrigt würde, und dann war der Körper $\boldsymbol{M}$ vom Grade mn'. Da aber die Reihenfolge willkürlich ist, so hätte man auch den Körper $\boldsymbol{A}$ zu Grunde legen und die Gleichung (B) in $\boldsymbol{A}$ bis auf einen gewissen Grad reductibel annehmen können. Dann hätte sich aber derselbe Körper $\boldsymbol{M}$ als kleinstes gemeinschaftliches Multiplum ergeben müssen; es wäre also auf Grund der Gleichung (10) die Gleichung (B) auf den m'^{ten} Grad erniedrigt werden. Also der Satz:

Wenn die im Körper R der rationalen Zahlen irreductibele Gleichung n^{ten} Grades (A) nach Adjunction einer Wurzel der im Körper R irreductibelen Gleichung m^{ten} Grades (B) auf den n'^{ten} Grad erniedrigt wird, so wird die Gleichung (B) nach Adjunction einer Wurzel der Gleichung (A) auf den m'^{ten} Grad erniedrigt, wobei $mn' = m'n$ ist.

Bleibt also die eine Gleichung irreductibel, so thut es auch die andere; und ebenso werden beide Gleichungen zugleich reductibel.

4. Da die Function $F(x,\beta)$ im Körper $\boldsymbol{B}$ irreductibel ist, so muss die Function $h(x)$ durch $F(x,\beta)$ theilbar sein:

$$h(x) = F(x,\beta)\ U(x,\beta),$$

und diese Identität in Beziehung auf x, welche zunächst nur für eine Wurzel β der Gleichung $g(x) = 0$ besteht, muss wegen der Irreductibilität dieser Gleichung im Körper R der rationalen Zahlen für alle m Wurzeln bestehen. Bezeichnen wir also die m Wurzeln der Gleichung $g(x) = 0$ mit $\beta', \beta'', \ldots \beta^{(m)}$; so ist

$$(11)\quad \begin{cases} h(x) = F(x,\beta')\ U(x,\beta') \\ h(x) = F(x,\beta'')\ U(x,\beta'') \\ \cdots\cdots\cdots\cdots\cdots \\ h(x) = F(x,\beta^{(m)})\ U(x,\beta^{(m)}); \end{cases}$$

folglich durch Multiplication

$$h(x)^m = F(x,\beta') F(x,\beta'') \ldots F(x,\beta^{(m)}) \\ \times U(x,\beta') U(x,\beta'') \ldots U(x,\beta^{(m)});$$

und da jeder der beiden Factoren $F(x,\beta') \ldots F(x,\beta^{(m)})$ und $U(x,\beta') \ldots U(x,\beta^{(m)})$ symmetrisch in Beziehung auf $\beta', \beta'', \ldots \beta^{(m)}$ ist und somit rationale Coefficienten hat, so muss wegen der Irreductibilität von $h(x)$ jeder derselben eine Potenz dieser Function sein, und zwar ergiebt die Gradvergleichung auf Grund der Gleichung (10)

$$(12) \begin{cases} F(x,\beta') F(x,\beta'') \ldots F(x,\beta^{(m)}) = h(x)^{m'} \\ U(x,\beta') U(x,\beta'') \ldots U(x,\beta^{(m)}) = h(x)^{m-m'}. \end{cases}$$

Die erste dieser Gleichungen zeigt Folgendes: Jede der Gleichungen $F(x,\beta^{(i)}) = 0$ $(i = 1, \ldots m)$ hat von den n Wurzeln der Gleichung $h(x) = 0$

$$\alpha', \alpha'', \ldots \alpha^{(n)}$$

nur n' zu Wurzeln, wobei $n' \leq n$ ist. Wir ordnen also die mn' Wurzeln aller dieser Gleichungen in ein Tableau, je nach der Wurzel β, zu der sie gehören:

$$(13) \begin{cases} \beta': & \alpha^{(k_1')}, & \alpha^{(k_2')}, & \ldots & \alpha^{(k_{n'}')} \\ \beta'': & \alpha^{(k_1'')}, & \alpha^{(k_2'')}, & \ldots & \alpha^{(k_{n'}'')} \\ \vdots & \vdots & \vdots & & \\ \beta^{(m)}: & \alpha^{(k_1^{(m)})}, & \alpha^{(k_2^{(m)})}, & \ldots & \alpha^{(k_{n'}^{(m)})}. \end{cases}$$

Hierbei bedeuten die oberen Indices gewisse n' Zahlen aus der Reihe 1 bis n. Auf Grund der Gleichung (12) kommt in diesem Tableau jede Wurzel α und zwar jede gleichvielmal, nämlich m' mal vor. Wir erhalten also $p = mn' = m'n$ Combinationen von Wurzeln β und Wurzeln α, und zwar gehören zu jeder Wurzel β n' Wurzeln α, und zu jeder Wurzel α m' Wurzeln β, wodurch jetzt wieder die Symmetrie wiederhergestellt ist, welche wegen der Gleichberechtigung der Körper A und B herrschen muss. Uebrigens ist es klar, dass diese p Combinationen gerade auch diejenigen sind, welche die p Wurzeln der Gleichung $f(x) = 0$ constituiren, die den Körper M bestimmt; denn entwickelt man die Function $f(a\alpha + b\beta)$ nach Taylor, so muss dieselbe wegen der Irreductibität von $F(x,\beta)$ für alle n' Werthe

α verschwinden, die zu einem und demselben Werthe β gehören; und da die Wurzel β hier ganz unbestimmt gelassen ist, so muss die Function für alle diejenigen Werthe $a\alpha + b\beta$ verschwinden, welche zu irgend einer der durch das Tableau (12) vorgezeichneten p Combinationen (β,α) gehören. — Diese letzten Betrachtungen unterscheiden sich dadurch charakteristisch von den vorhergehenden, dass in ihnen nicht mehr bloss eine Wurzel einer irreductibelen Gleichung und der zugehörige Körper, sondern dass das ganze System von Wurzeln, die eine Gleichung befriedigen, in Betracht gezogen ist. In der That ist es für eingehendere Untersuchung erforderlich, das Verhältniss der auftretenden Systeme von Wurzeln und der zugehörigen Körper zu einander festzustellen; und zwar führen wir die Untersuchung dieser Verhältnisse in der Dedekind'schen Auffassung der Abbildungen oder Permutationen der Körper durch.

8. (D. § 163; B. § 16.) Wenn man ein Gesetz festlegt, nach welchem jeder Zahl ω eines Zahlkörpers Ω eine bestimmte Zahl ω' entspricht, so bezeichnen wir diesen Prozess als eine Abbildung des Körpers Ω und nennen die Zahl ω' das Bild der Zahl ω. Wir fragen nun: ist es möglich, einen Zahlkörper Ω so abzubilden, dass alle rationalen Beziehungen zwischen den Zahlen ω sich vollständig auf ihre Bilder ω' übertragen? Giebt es derartige Abbildungen, so sollen sie Permutationen des Körpers Ω heissen. Dazu ist nothwendig und in jedem Falle auch hinreichend, dass, wenn α und β irgend zwei Zahlen des Körpers Ω sind und mit dem Zeichen o wieder eine beliebige von den vier rationalen Rechenoperationen bezeichnet wird, das Bild von $\alpha o \beta$ gleich $\alpha' o \beta'$ ist, oder:

$$(1)\quad (\alpha + \beta)' = \alpha' + \beta'$$
$$(2)\quad (\alpha - \beta)' = \alpha' - \beta'$$
$$(3)\quad (\alpha\beta)' = \alpha'\beta'$$
$$(4)\quad \left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta}.$$

Aber diese vier Bedingungen sind sogar mehr als hinreichend; in der That ist leicht zu zeigen, dass das Bestehen der Gleichungen (1) und (3) für beliebige α und β das Be-

stehen der Gleichungen (2) und (4) nach sich zieht. Uebrigens verlangt die dritte Gleichung, dass das Bild einer von Null verschiedenen Zahl β ein von Null verschiedenes ist; denn sonst würde das Bild jeder Zahl verschwinden, und dieser Fall kann füglich ausgeschlossen werden. Hieraus folgt auf Grund der zweiten Gleichung, dass verschiedene Zahlen α und β auch verschiedene Bilder haben und dass die hier vollzogene (bis jetzt noch hypothetische) Abbildung eine umkehrbar eindeutige sein muss. Nun bilden aber die Bilder aller Zahlen ein System von Zahlen Ω', welches ein Körper sein muss, weil ihm die charakteristischen Eigenschaften des Körpers zukommen; denn die Zahl $\alpha' \circ \beta'$ ist das Bild von $\alpha \circ \beta$, also einer in Ω enthaltenen Zahl und muss demzufolge in dem System Ω' auftreten. Auf Grund der umkehrbaren Eindeutigkeit kann man daher jeder Zahl des Körpers Ω' diejenige bestimmte Zahl ω des Körpers Ω zuordnen, deren Bild sie war; und diese Abbildung ist eine Permutation, weil ihr, wie leicht zu erweisen, die charakteristischen Eigenschaften (1) — (4) zukommen. Jede Permutation eines Körpers lässt sich also durch die umgekehrte oder inverse Permutation wieder zurücknehmen oder in die identische Permutation, d. h. in diejenige Permutation verwandeln, durch welche jede Zahl in sich selbst abgebildet wird. Bezeichnen wir, wie üblich, die successive Anwendung zweier Operationen als symbolisches Product, die identische Permutation durch das Symbol 1, so können wir dies so ausdrücken:

$$P\,P^{-1} = 1.$$

Was diese symbolische Multiplication angeht, so ist wohl zu beachten: ist P diejenige Permutation, welche den Körper Ω in Ω', Q diejenige Permutation, welche den Körper Ω' in Ω'', R diejenige Permutation, welche den Körper Ω'' in Ω''' überführt, so führt PQ Ω in Ω'' und folglich (PQ)R Ω in Ω''' über; ebenso führt QR Ω' in Ω''' und folglich P(QR) Ω in Ω''' über. Es gilt also das associative Gesetz:

$$(PQ)R = P(QR).$$

Das commutative Gesetz [PQ = QP] gilt aber im allgemeinen schon darum nicht, weil Q zunächst nur als

Permutation des Körpers Ω' und gar nicht als Permutation des Körpers Ω Bedeutung hat.

Setzt man in der vierten der obigen Gleichungen $\beta = \alpha$, so findet man, dass die Zahl 1 und folglich der Körper der rationalen Zahlen durch jede Permutation des Körpers Ω in sich selbst abgebildet wird. Von einem beliebigen Divisor des Körpers Ω lässt sich jedenfalls soviel aussagen, dass er in einen Divisor des Körpers Ω' permutirt wird. Genügt ferner die Zahl Θ, die dem Körper Ω angehört, einer Gleichung n^{ten} Grades mit rationalen Coefficienten, so muss wegen der Erhaltung der rationalen Beziehungen die Zahl Θ', die das Bild von Θ ist, derselben Gleichung genügen, also auch eine Wurzel jener Gleichung sein.

Diese letzte Bemerkung zeigt uns, wenn wir nunmehr von der Untersuchung eines beliebigen zu der eines endlichen Körpers n^{ten} Grades übergehen, dass ein solcher überhaupt nur n Permutationen haben kann. Wird nämlich der Körper Ω vom Grade n durch die Wurzel Θ der Gleichung $f(\Theta) = 0$ constituirt, so muss durch eine beliebige Permutation Θ in eine der n Wurzeln dieser Gleichung übergehen, und sobald dieselbe festgelegt, geht jede rationale Function von Θ mit rationalen Coefficienten in dieselbe rationale Function der Zahl Θ', die das Bild von Θ ist, über. Ordnen wir aber umgekehrt der Zahl Θ, die den Körper Ω constituirt, eine der n Zahlen Θ' zu, die derselben irreductibelen Gleichung n^{ten} Grades genügt wie Θ, und jeder beliebigen Zahl ω von Ω diejenige Zahl ω', welche durch dieselben rationalen Operationen aus Θ' gebildet ist, durch welche ω aus Θ gebildet werden kann, so stellt diese Zuordnung jedenfalls eine Abbildung des Körpers Ω in dem am Eingange des Paragraphen besprochenen Sinne dar, und die Abbildung ist eine Permutation, weil ihr, wie leicht zu beweisen ist, die durch die Gleichungen (1) und (3) geforderten Eigenschaften zukommen. Wir haben also den Satz:

Jeder endliche Körper n^{ten} Grades hat n verschiedene Permutationen, von denen eine stets die identische Permutation ist. Jede dieser n Permutationen wird dadurch völlig bestimmt, dass man

einer constituirenden Zahl Θ des Körpers eine Zahl Θ' zuweist, welche derselben irreductibelen Gleichung n^{ten} Grades wie Θ genügt.

Jeder Zahl ω des Körpers Ω werden durch die n verschiedenen Permutationen dieses Körpers n (gleiche oder verschiedene) Zahlen $\omega', \omega'', \ldots \omega^{(n)}$ resp. der Körper $\Omega', \Omega'', \ldots \Omega^{(n)}$ zugeordnet; diese n Zahlen bezeichnet man als die der Zahl ω conjugirten Zahlen, ihr Product als die Norm von ω; in Zeichen

$$(5) \quad N(\omega) = \omega' \omega'' \ldots \omega^{(n)};$$

und diese Definition lehrt unmittelbar, dass die Norm eines Productes gleich dem Producte der Normen ist:

$$(6) \quad N(\alpha\beta) = N(\alpha)\, N(\beta).$$

Neben dem Begriffe der Norm ist noch der Begriff der Discriminante von besonderer Wichtigkeit für die Theorie der endlichen Körper; hat man nämlich an einem Körper n^{ten} Grades ein System von n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ und bildet man das Quadrat der Determinante, welche aus den n.n Bildern dieser Zahlen zusammengesetzt ist:

$$\Sigma \pm \alpha_1' \alpha_2'' \ldots \alpha_n^{(n)},$$

so bezeichnet man dasselbe als die Discriminante der n Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$ und schreibt es

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Jede Norm und jede Discriminante ist auf Grund des Fundamentalsatzes der symmetrischen Functionen eine rationale Zahl. Ist Θ constituirende Zahl des Körpers, so ist die Discriminante der n ersten Potenzen dieser Zahl

$$\Delta(1, \Theta, \Theta^2, \ldots \Theta^{n-1})$$

bekanntlich gleich dem Quadrat des Productes der $\frac{n.(n-1)}{1.2}$ Differenzen, welche man aus den Combinationen der Wurzeln $\Theta', \Theta'', \ldots \Theta^{(n)}$ zu zweien erhält, und somit von Null verschieden, weil eine irreductibele Gleichung nicht zwei gleiche Wurzeln haben kann. Hieraus folgt leicht, dass die Discriminante irgend eines Systemes von n Zahlen verschwindet oder nicht verschwindet, je nachdem diese Zahlen ein ab-

hängiges oder unabhängiges System bilden. Jedes System von n Zahlen, dessen Discriminante von Null verschieden ist, bildet also eine Basis des Körpers. (§§ 2, 3.)

9. Durch jede der n Abbildungen eines Körpers Ω vom Grade n wird auch eine ganz bestimmte Abbildung eines Divisors A, der den Grad m hat, vermittelt. Da aber der Körper A nur m Permutationen zulässt, so muss nothwendig, wenn $m < n$, also A ein echter Theiler ist, zu zwei verschiedenen Permutationen von Ω eine und dieselbe Permutation von A gehören, und dieser Punkt muss vor allem jetzt bis zu einem gewissen Umfange aufgehellt werden. Ist Θ constituirende Zahl des Körpers Ω, α constituirende Zahl des Divisors A und ist $\alpha = \varphi(\Theta)$, wobei $\varphi(\Theta)$ eine ganze Function von Θ mit rationalen Coefficienten bedeutet, so genügt α einer irreductibelen Gleichung des Grades m: $g(\alpha) = 0$, deren höchster Coefficient, wie gewöhnlich, die Eins sein mag. Die Function

$$(1)\quad [z-\varphi(\Theta')]\,[z-\varphi(\Theta'')]\ldots.[z-\varphi(\Theta^{(n)})] = f(z),$$

deren Coefficienten rationale Zahlen sind, ist reductibel, wenn $m < n$ ist; da aber jede irreductibele Function, welche durch eine der n conjugirten Grössen $\alpha' = \varphi(\Theta')$, $\alpha'' = \varphi(\Theta'')$, ... $\alpha^{(n)} = \varphi(\Theta^{(n)})$ annullirt wird, nothwendigerweise auch alle verschiedenen unter diesen Grössen zu Wurzeln haben muss, so kann jeder irreductibele Factor von f(z) immer nur g(z) sein, und folglich ist, wenn $\frac{n}{m} = p$ gesetzt wird,

$$(2)\quad f(z) = [g(z)]^p. \text{ *)}$$

Uebrigens kann man die Function f(z) auch auf folgendem Wege erhalten: ist $\omega_1, \omega_2, \ldots, \omega_n$ eine beliebige Basis des Körpers Ω und α eine beliebige Zahl desselben, so ist $\alpha\omega_i$ ($i = 1, \ldots n$) auch eine Zahl des Körpers Ω, also:

$$(3)\quad \alpha\omega_i = \Sigma_k c_{ik}\omega_k\,,\,{}^{i}_{k}\} = 1,\ 2,\ \ldots\ n,$$

wobei die Coefficienten c rationale Zahlen sind. (§ 3.) Da aber bei jeder Permutation die rationalen Beziehungen un-

*) Schönemann, Grundzüge einer allgemeinen Theorie der höheren Congruenzen, Crelles J. Bd. 31, S. 273, § 4.

geändert bleiben, so genügen die n Bilder von α der Gleichung n^{ten} Grades in Determinantenform:

$$(4) \quad | c_{ik} - z\delta_{ik} | = 0, \qquad \begin{matrix} i \\ k \end{matrix} \} = 1, 2, \ldots n,$$

in welcher δ_{ik} das Kronecker'sche Symbol, nämlich eine Zahl bedeutet, welche Null oder Eins ist, je nachdem die Indices i und k verschieden oder gleich sind. Welche Zahl also auch $\alpha = \varphi(\Theta)$ sein möge, immer ist

$$(5) \begin{cases} (z - \alpha')(z - \alpha'') \ldots (z - \alpha^{(n)}) \text{ oder} \\ (z - \varphi(\Theta'))(z - \varphi(\Theta'')) \ldots (z - \varphi(\Theta^{(n)})) \equiv (-1)^n |c^{ik} - z\delta^{ik}|. \end{cases}$$

Hieraus folgt für $z = 0$, dass

$$(6) \quad | c^{ik} | = N(\alpha) \qquad \begin{matrix} i \\ k \end{matrix} \} = 1, 2, \ldots n.$$

ist.

Nach dieser kurzen Abschweifung kehren wir wieder zur Gleichung (2) zurück; dieselbe lehrt uns, dass zu p verschiedenen Abbildungen des Körpers Ω immer dieselbe Abbildung des Körpers A gehört und dass es insbesondere unter den Abbildungen des Körpers Ω p geben wird, durch welche der Körper A identisch permutirt wird. Dass eine rationale Zahl n gleiche und dass eine constituirende Zahl n verschiedene Bilder hat, ist nur ein Specialfall dieses Satzes. Weiss man also nur, welcher Permutation der Divisor A unterliegt, so ist die Permutation des Multiplums Ω noch nicht mitgegeben, sondern noch p-fach unbestimmt.

Hat man nun zwei Körper A und B resp. von den Graden n und m und sind α und β constituirende Zahlen dieser Körper, so zeigen die Ausführungen der §§ 6 und 7, dass ihr kleinstes gemeinschaftliches Multiplum M, welches den Grad $p = nm' = mn'$ hat, durch eine mit rationalen Zahlen a und b gebildete Verbindung $a\alpha + b\beta$ constituirt werden kann, und dass die p Wurzeln der irreductibelen Gleichung, welcher diese Verbindung genügt, durch p Combinationen der n Bilder α und der m Bilder β erzeugt werden. Das Multiplum M unterliegt also in seiner Eigenschaft als Körper p verschiedenen Permutationen, bei deren Anwendung die Theiler A und B nach dem Vorhergehenden in bestimmter Weise mitpermutirt werden; und zwar wird ein und dieselbe Permutation des Körpers A bei m', ein und dieselbe

Permutation des Körpers B bei n' Permutationen des Körpers M auftreten. Eine solche Permutation des Körpers M, insofern sie als eine und dieselbe, auf die beiden Körper A und B zugleich zugleich angewendete Abbildung betrachtet wird, mag eine simultane Permutation der Körper A und B heissen. Da jede Permutation die Eigenschaft der Eindeutigkeit hat, so ist es ersichtlich, dass bei jeder simultanen Permutation der Körper A und B ihr grösster gemeinschaftlicher Divisor Δ einer und derselben Permutation unterworfen wird; ob aber diese nothwendige Bedingung auch die hinreichende ist, d. h. ob zu irgend zwei Permutationen von A und B, welche eine und dieselbe Permutation des grössten gemeinschaftlichen Theilers Δ zur Folge haben, auch eine Permutation des kleinsten gemeinschaftlichen Multiplums M gehört, ist eine Frage von grossem Interesse, deren Beantwortung mir bis jetzt noch nicht hat gelingen wollen; übrigens ist dieselbe für die Lösung unserer Aufgabe nicht nothwendig.

Ein Körper Ω des Grades n liess n Permutationen zu, von welchen eine die identische Permutation war, während die anderen Permutationen immer nur einen Theiler des Körpers Ω in sich selbst überführen konnten. Damit ist aber keineswegs gesagt, dass die durch die nichtidentischen Permutationen erzeugten Körper alle von Ω verschieden sein müssten. Wie dem aber auch sein möge, jedenfalls lässt jeder der $n-1$ durch die nicht identische Permutation erzeugten Körper auch für sich wieder je n verschiedene Permutationen zu. Um zu erkennen, wie diese Permutationen unter einander nnd mit den n Permutationen des Körpers Ω in Beziehung zu setzen sind, führen wir zunächst den Begriff des Normalkörpers ein.

Wenn ein Körper N, der den Grad N hat, durch seine N Permutationen in N conjugirte Körper übergeführt wird, welche ihrem Zahleninhalte nach mit N sämmtlich identisch sind, so heisst der Körper ein Normalkörper oder Galois'scher Körper. Ist Θ eine constituirende Zahl des Normalkörpers N, so ist folglich jede der N zu Θ conjugirten Zahlen eine ganze rationale Function von Θ mit rationalen Coefficienten:

(1) $\Theta' = \varphi'(\Theta),\ \Theta'' = \varphi''(\Theta),\ \ldots .\ \Theta^{(N)} = \varphi^{(N)}(\Theta).$

Ist umgekehrt Θ constituirende Zahl eines Körpers N und sind die N zu Θ conjugierten Zahlen sämmtlich in N enthalten, [d. h. bestehen Formeln der Form (1)], so ist N ein Normalkörper. Ein Normalkörper hat die charakteristische Eigenschaft, dass mit jeder seiner Permutationen auch die entsprechenden Permutationen der conjugirten Körper gleich mitbestimmt sind; denn die conjugirten Körper haben ja denselben Zahleninhalt wie jener. Hieraus folgt, dass man in diesem Falle ohne weiteres auf einen beliebigen conjugirten Körper zu N eine der Permutationen von N anwenden oder, wenn man die Permutationen von N mit

(2) $P', P'', \ldots . P^{(N)}$

bezeichnet, dass man irgend zwei dieser Permutationen ohne weiteres hinter einander auf N ausüben kann. Da aber nach § 8 auf diesem Wege immer wieder nur eine Permutation von N entstehen kann, so ist das Product irgend zweier Permutationen der Reihe (2) wieder eine Permutation dieser Reihe. Wenn eine endliche oder unendliche Anzahl von Operationen diese Eigenschaft besitzt, dass die successive Anwendung irgend zweier der in Rede stehenden Operationen wieder eine solche Operation ist, so pflegt man die Gesammtheit dieser Operationen als eine Gruppe von Operationen (nach Galois) zu bezeichnen, und wenn die Anzahl der Operationen eine endliche ist, so nennt man dieselbe die Ordnung der Gruppe. Also haben wir den Satz:

Die Permutationen eines Normalkörpers des Grades N bilden eine Gruppe der Ordnung N.

Diesem Satze können wir mit Hilfe des Begriffes des holoedrischen Isomorphismus noch andere Fassungen ertheilen, welche den Zusammenhang des hier gewählten Gruppenbegriffes mit der etwas üblicheren, einschränkenderen Begriffsformulirung vermitteln.*) Wenn nämlich zwei Gruppen von

*) Ueber die hier gewählte Auffassung des holoedrischen Isomorphismus und der Gruppe s. Klein, Vorlesungen über das Ikosaeder, Leipzig, 1884, Abschn. I, Cap. I, § 2. Vergl. zum folg. auch Abschn. I, Cap. IV, §§ 2—4.

Operationen G und G′ in der Weise in Correspondenz gesetzt sind, dass jeder Operation der Gruppe G eine oder mehrere Operationen der Gruppe G′ entsprechen und dass dem Producte zweier Operationen von G das Product entsprechender Operationen von G′ entspricht, so nennt man die Gruppen isomorph. Wenn insbesondere die Correspondenz zwischen G und G′ eine eineindeutige ist, so haben die Gruppen gleiche Ordnungen und so bezeichnet man den Isomorphismus als holoedrisch oder einstufig; dann sind die Gruppen, wenn man von dem Inhalt der Operationen absieht und nur noch die Operationen selbst und die Beziehungen, in welche sie durch Multiplication treten, berücksichtigt, überhaupt identisch und können daher im Sinne der Gruppentheorie als Eins betrachtet werden. Wenn aber einer Operation von G mehr als eine, nämlich m Operationen von G′ correspondiren, so heisst der Isomorphismus meriedrisch oder mehrstufig; in diesem Falle ergiebt eine Tabellenbildung, deren Princip man leicht aus der Exhaustionsmethode des § 4 entnehmen kann, dass jeder Operation von G eine gleiche Anzahl von Operationen aus G′ entspricht; daher ist die Ordnung von G′ das m fache der Ordnung von G und der Isomorphismus kann als m-stufig bezeichnet werden. Von besonderem Interesse sind die m Operationen von G′, welche der identischen Operation von G entsprechen; diese haben auf Grund des Begriffes des Isomorphismus für sich Gruppencharakter, d. h. sie bilden eine Untergruppe der Ordnung m von G′. Enthält diese Untergruppe die Operationen

$$(3)\quad P', P'', \ldots P^{(m)},$$

ist P ferner irgend eine Operation von G′ und bildet man die Operationen:

$$(4)\quad P^{-1}P'P,\ P^{-1}P''P, \ldots P^{-1}P^{(m)}P,$$

so constituiren diese m Operationen wieder eine Gruppe, welche man (im allgemeinen Falle) als die Transformirte der Gruppe (3) durch P zu bezeichnen pflegt. In dem hier besprochenen Falle ergiebt sich dann das merkwürdige Verhältniss, dass die Operationen (4), von der Reihenfolge abgesehen, mit den Operationen (3) übereinstimmen; bei mehr-

stufigem Isomorphismus wird also die Untergruppe, welche der identischen Operation von G entspricht, durch jede Operation von G in sich selbst transformirt, oder, wie man sagt, sie bildet eine ausgezeichnete Untergruppe von G.

Es seien nun die N Wurzeln der Gleichung N^{ten} Grades, welche der Normalkörper N charakterisirt, wie vorher:

$$(5)\quad \Theta', \Theta'', \ldots \Theta^{(n)},$$

so erhalten wir bei Anwendung der N Permutationen des Körpers N N verschiedene Anordnungen oder Complexionen*) der Wurzeln Θ; denn bei jeder Permutation treten auch wieder alle N Wurzeln als Bilder auf, weil verschiedene Zahlen verschiedene Bilder haben. Zu jeder Permutation des Körpers gehört also eine bestimmte Complexion der Wurzeln Θ, und die Permutation des Normalkörpers ist also mit einer gewissen Vertauschung oder Substitution der Wurzeln Θ holoedrisch isomorph. Dabei entspricht natürlich der identischen Permutation die identische Substitution, d. h. diejenige Substitution, bei welcher alle Wurzeln ihre Stelle behalten. In dieser Gruppe von Vertauschungen der Wurzeln haben wir also ein vollständiges Bild jener Operationen, die wir Permutationen genannt haben. Wir können aber von der Substitutionengruppe auf Grund der vorher entwickelten Begriffe sogleich folgendes aussagen: Erstens: keine der N Substitutionen ausser der Identität lässt irgend eine der N Wurzeln Θ an ihrer Stelle. Zweitens: es ist stets möglich, eine beliebige Wurzel Θ mit einer beliebigen anderen zu vertauschen, wie ohne weiteres aus demjenigen folgt, was wir über das Wesen der Permutation in § 8 erkannt haben; diese Eigenschaft bezeichnet man als Transitivität der Substitutionengruppe. Drittens: Die Gruppe ist einfach transitiv, d. h. es ist nicht möglich, irgend zwei beliebige Elemente auf zwei beliebige folgen zu lassen; denn sobald bekannt ist, in welche Wurzel irgend eine der

*) Ich wähle den Ausdruck „Complexion" statt der üblicheren „Permutation", um die Permutation, die hier eine Operation ist, von der Complexion, welche ein Ergebniss dieser Operation ist, sicher unterscheiden zu können.

Zahlen der Reihe (5) übergeführt werden soll, ist die Permutation des Körpers und mit ihr die zugehörige Substitution der Wurzeln völlig bestimmt. Schliesslich sei bemerkt, dass man der besprochenen Thatsache noch eine dritte Seite abgewinnen kann. Ist nämlich Θ wieder eine beliebige der N Wurzeln der Reihe (5), so ist auf Grund der Relation (1) und auf Grund der Erhaltung der rationalen Beziehungen (§ 8) diejenige Abbildung $P^{(r)}$, welche Θ in $\Theta^{(r)}$ überführt, aequivalent mit der Complexion

$$\left.\begin{array}{ll} & \varphi'(\Theta^{(r)}),\ \varphi''(\Theta^{(r)}),\ \ldots\ \varphi^{(N)}(\Theta^{(r)}) \\ \text{oder} & \varphi'\varphi^{(r)}(\Theta),\ \varphi''\varphi^{(r)}(\Theta)\ \ldots\ \varphi^{(N)}\varphi^{(r)}(\Theta) \end{array}\right\} (6).$$

Folglich ist

$$(6)\varphi'\varphi^{(r)}(\Theta)=\varphi^{(\varrho_1)}(\Theta),\varphi''\varphi^{(r)}(\Theta)=\varphi^{(\varrho_2)}(\Theta),\ldots\varphi^{(N)}\varphi^{(r)}(\Theta)=\varphi^{(\varrho_N)}(\Theta),$$

wo die Indices $\varrho_1,\ \varrho_2,\ \ldots\ \varrho_N$ diejenige Complexion der Wurzelindices ist, welche zu der der Permutation $P^{(r)}$ holoedrisch entsprechenden Substitution gehört. Die Functionen, $\varphi', \varphi'', \ldots \varphi^{(N)}$ der Reihe (1) bilden folglich auch eine Gruppe, welche zu den beiden vorher besprochenen holoedrisch isomorph ist, — freilich nur in dem Sinne, dass die Werthe, welche sie für die Wurzeln Θ annehmen, ein im Sinne der Gruppentheorie abgeschlossenes Ganze ausmachen. Wir fassen die gewonnenen Anschauungen in dem Satze zusammen, indem wir noch, wie üblich, die Anzahl der Elemente, welche in eine Substitutionengruppe eingehen, als den Grad der Gruppe bezeichnen:

Der Gruppe der Permutationen eines Normalkörpers des Grades N entspricht holoedrisch isomorph eine einfach transitive Gruppe von Substitutionen, deren Gradzahl der Ordnungszahl N gleich ist und deren Operationen alle oder gar kein Element umsetzen, und ebenso holoedrisch isomorph eine Gruppe von Functionen. Die Elemente der Substitutionen sind die N constituirenden Zahlen der N conjugirten Körper, die Functionen sind solche N rationale Functionen mit rationalen Coefficienten, durch

welche alle N Wurzeln als Functionen einer von ihnen dargestellt werden können.*)

11. Wenden wir uns nunmehr zur Betrachtung eines beliebigen Körpers Ω des Grades n. Ist Θ constituirende Zahl des Körpers Ω und geht der Körper Ω durch die n zulässigen Permutationen in die conjugirten Körper

$$(1) \quad \Omega', \Omega'', \ldots \Omega^{(n)}$$

über, welche ihrem Zahleninhalte nach sehr wohl theilweise oder auch ganz identisch sein können und resp. die constituirenden Zahlen

$$(2) \quad \Theta', \Theta'', \ldots \Theta^{(n)}$$

besitzen, so ist das kleinste gemeinschaftliche Multiplum der Körper Ω', Ω'', $\ldots$ $\Omega^{(n)}$ ein Körper N, welcher die Norm des Körpers Ω heisst, und dessen Grad N sein möge. Die N Permutationen der Norm N sind (§ 9) zugleich die N simultanen Permutationen der Körper Ω', Ω'', $\ldots$ $\Omega^{(n)}$. Durch jede dieser Permutationen wird die Reihe der Zahlen (2) in eine gewisse andere Anordnung übergeführt; denn bei jeder Permutation kann irgend eine der Zahlen dieser Reihe immer nur in eine Zahl derselben Reihe übergehen, und da die Zahlen alle verschieden sind, so müssen auch ihre Bilder verschieden sein. (§ 8.) Den N verschiedenen Permutationen des Körpers N entsprechen also holoedrisch isomorph N verschiedene Complexionen der Zahlen (2):

$$(3) \quad \left\{ \begin{array}{llll} \Theta_1', & \Theta'', & \ldots\ldots & \Theta^{(n)} \\ \Theta^{(i_1')}, & \Theta^{(i_1'')}, & \ldots\ldots & \Theta^{(i_1^{(n)})}, \\ \ldots\ldots\ldots & & & \\ \Theta^{(i_{N-1}')}, & \Theta^{(i_{N-1}'')}, & \ldots & \Theta^{(i_{N-1}^{(n)})} \end{array} \right.$$

Der Körper N ist aber ein Normalkörper; denn nach § 7, 2 kann man die n rationalen Zahlen a', a'', $\ldots$ $a^{(n)}$ so bestimmen, dass

*) Netto, Substitutionentheorie, Leipzig, 1882, §§ 89—90, 122—124 (hier sind die möglichen Typen solcher Gruppen untersucht), 153. Camille Jordan, Traité des substitutions, Paris 1870, 69—71, 358.

$$(4)\quad \xi' = a'\Theta' + a''\Theta'' + a^{(n)}\Theta^{(n)}$$

constituirende Zahl wird; genügt dieselbe der irreductibelen Gleichung

$$(5)\quad \varphi(z) = 0,$$

so erhält man alle Wurzeln ξ', ξ'', $\ldots$ $\xi^{(N)}$ dieser Gleichung, indem man die Substitutionen (3) auf den Ausdruck (4) anwendet:

$$(6)\quad \begin{cases} \xi' = a'\Theta' + a''\Theta'' + \ldots + a^{(n)}\Theta^{(n)} \\ \xi'' = a'\Theta^{(i_1')} + a''\Theta^{(i_1'')} + \ldots + a^{(n)}\Theta^{(i_1^{(n)})} \\ \ldots\ldots\ldots\ldots \\ \xi^{(N)} = a'\Theta^{(i_{N-1}')} + a''\Theta^{(i_{N-1}'')} + \ldots + a''\Theta^{(i_{N-1}^{(n)})}; \end{cases}$$

da also alle Bilder von ξ' wieder dem Körper N angehören, so ist N ein Normalkörper.

Die Gruppe seiner Permutationen, welche wir vorhin besprochen haben, nennen wir die Gruppe des Körpers Ω; die ihr holoedrisch isomorph gegenüberstehende Gruppe von Vertauschungen, welche durch das Tableau (3) charakterisirt wird, ist es, welche man gewöhnlich als die Gruppe der die Wurzeln Θ definirenden Gleichung zu bezeichnen pflegt, während man den Ausdruck (3) die Galois'sche Resolvente nennt. In dieser letzten Auffassung hat die Gruppe den Grad n und die Eigenschaft der Transitivität; denn man kann jeden Körper der Reihe (8) in jeden anderen permutiren.*) Da diese Gruppe von Vertauschungen eine Untergruppe der Gruppe aller überhaupt möglichen Vertauschungen der Grössen Θ', Θ'', $\ldots$ $\Theta^{(n)}$ ist, so ist die Ordnung N, welche nach § 4 ein Multiplum von n ist, ein Theiler von n!. Ist $N = n$, so ist der Körper Ω ein Normalkörper, denn er ist alsdann seine eigene Norm; ist $N = n!$, so ist er ein allgemeiner Körper, d. h. ein Körper, welcher sich hinsichtlich seiner Eigenschaften ganz so verhält, wie ein Körper, welcher durch eine Gleichung n^{ten} Grades mit unbestimmt gelassenen Coefficienten definirt wird. Wendet man die Permutationen

*) Die Transitivität der Gruppe ist (nach Cauchy) mit der Irreductibilität der Gleichung untrennbar verbunden; Netto l. c. § 154, Jordan l. c. 357.

der Gruppe des Körpers Ω auf das System der constituirenden Zahlen (6) an, so erhält man auf Grund der Erörterungen des vorigen Paragraphen im Ganzen N verschiedene Complexionen der Zahlen ξ; daher ist unsere Permutationsgruppe mit einer zweiten Gruppe von Vertauschungen holoedrisch isomorph, deren Grad aber jetzt N ist und welche dieselben Eigenschaften besitzt, wie die Gruppe des vorigen Paragraphen. Schliesslich kann man auch wieder der Permutationsgruppe eine Gruppe von Functionen zuordnen; doch übergehen wir dies, weil es für uns hier kein wesentliches Interesse darbietet. Wir haben den Satz:

Wenn die Norm N des Körpers Ω vom n^{ten} Grade den Grad N hat, der ein Multiplum von n und ein Theiler von n! ist, so kann man N simultane Permutationen auf die n Bilder des Körpers Ω anwenden, welche eine Gruppe bilden. Diese Gruppe des Körpers Ω ist mit einer Gruppe von Vertauschungen der n constituirenden Zahlen der n conjugirten Körper und mit einer Gruppe von Vertauschungen der N conjugirten constituirenden Zahlen des Normalkörpers N holoedrisch isomorph.

12. Es sei, wie vorher, N ein Normalkörper vom Grade N und Ω irgend ein Theiler des Grades n, so dass also N nicht gerade die Norm des Körpers zu sein braucht, sondern auch ein Multiplum der Norm sein kann. Dann habe von den N Permutationen des Körpers N in sich $\frac{N}{n}$ die Eigenschaft, dass sie den Körper Ω identisch permutiren. Diese $p = \frac{N}{n}$ Permutationen haben also für sich Gruppencharakter; d. h. sie bilden eine Untergruppe U der Gruppe G der Permutation des Normalkörpers N. Von grösster Wichtigkeit für uns ist aber, dass dieses Verhältniss sich umkehren lässt: Wenn die Gruppe G des Normalkörpers N eine Untergruppe U der Ordnung p besitzt, so bilden alle diejenigen Zahlen von N, welche durch alle p Permutationen der Untergruppe und durch keine andere Permutation von G identisch permutirt werden, einen Divisor von N, der den Grad $n = \frac{N}{p}$

hat. Denn sind α und β irgend zwei Zahlen von N, welche durch die p Permutationen der Untergruppe U identisch permutirt werden und führen wir wieder das Zeichen o ein, so wird auf Grund des Begriffes der Permutation (§ 8) das Bild der Zahl $\alpha o \beta$ bei allen p Permutationen von U wieder $\alpha o \beta$ sein und folglich auch zu dem charakterisirten Systeme von Zahlen gehören; unser System Ω ist also ein Körper und zwar ein Divisor von N. Da wir ferner angenommen haben, dass die Zahlen des Körpers Ω auch nur bei den Permutationen der Untergruppe U sämmtlich ungeändert bleiben, so wird jede weitere Permutation von G den Körper Ω nicht-identisch permutiren; und zwar bilden wir zur Feststellung dieser Verhältnisse in bekannter Weise eine Tabelle:

$$(T)\begin{cases} P' = 1,\ P'',\ P''' \ldots P^{(p)} \\ S'',\ P''S'',\ P'''S'' \ldots P^{(p)}S'' \\ \ldots\ldots\ldots\ldots\ldots \\ S^{(n)},\ P''S^{(n)},\ P'''S^{(n)} \ldots P^{(p)}S^{(n)}. \end{cases}$$

Hierin giebt die erste Zeile die Permutationen der Untergruppe U; ist S'' irgend eine nicht-identische Permutation für Ω, so sind alle Permutationen von einander und von den Operationen der ersten Zeile verschiedene Operationen und üben sämmtlich und auch ausschliesslich auf den Körper Ω die gleiche Wirkung aus; ebenso ist S''' eine Operation, welche unter den vorher hingeschriebenen noch nicht vorkommt u. s. w. Hieraus folgt, dass der Körper Ω den Grad n hat und dass die Operationen 1, S'', ... $S^{(n)}$ als seine Permutationen betrachtet werden können; w. z. b. w. Von Interesse ist es zu sehen, wie aus der Untergruppe U, die den Körper Ω bestimmt, die entsprechenden Untergruppen für alle zu Ω conjugirten Körper

$$\Omega', \Omega'', \ldots \Omega^{(n)}$$

gefunden verden können. Nehmen wir an, dass der Körper Ω durch die identische Operation in Ω' und durch die Operation $S^{(r)}$ (r = 1, 2, ... n) in den Körper $\Omega^{(r)}$ übergeführt werde, so wird $\Omega^{(r)}$ durch die Operationen

$$1,\ S^{(r)-1}P''S^{(r)},\ S^{(r)-1}P'''S^{(r)} \ldots S^{(r)-1}P^{(p)}S^{(r)},$$

und, wie man leicht erkennt, auch nur durch diese identisch

permutirt werden. Man erhält also diejenige Untergruppe, welche dieselbe Bedeutung für $\Omega^{(r)}$ hat, wie $U = U'$ für $\Omega = \Omega'$, indem man die Untergruppe U durch eine derjenigen Permutationen von N transformirt, welche Ω in $\Omega^{(r)}$ überführen. Insbesondere kann es vorkommen, dass alle diese transformirten Gruppen mit der ursprünglichen Gruppe identisch ausfallen; dann ist die Untergruppe eine ausgezeichnete Untergruppe und der Divisor Ω kann passend ein ausgezeichneter Divisor genannt werden. Derartige ausgezeichnete Untergruppen und Divisoren spielen in der Theorie der Gleichungen eine besondere Rolle; für uns genügt aber hier das allgemeine Ergebniss, das wir in den Satz zusammenfassen:

Ist in der Gruppe G der Permutationen eines Normalkörpers N des Grades N eine hinreichend ausgedehnte Untergruppe U der Ordnung $p = \frac{N}{n}$ enthalten, so bilden alle Zahlen, welche durch alle Permutationen der Untergruppe identisch abgebildet werden, einen Theilkörper Ω des Grades n. Die entsprechenden Untergruppen, welche für die conjugirten Körper zu Ω dieselbe Rolle spielen, wie U für Ω, erhält man aus U durch Transformation.

13. Die hier zuletzt auseinandergesetzten Sätze über die Permutationen der Körper überhaupt und der Normalkörper insbesondere sind nur einige wenige Theoreme der modernen Theorie der Gruppen, welche gegenwärtig wegen ihrer zahlreichen Beziehungen zu mancherlei sehr verschiedenartigen Disciplinen im Mittelpunkte des mathematischen Interesses steht, nämlich diejenigen Theoreme, welche wir im folgenden brauchen werden und welche bei einer einigermassen eindringenderen Behandlung der Theorie der Zahlkörper nothwendig zu sein schienen. Abweichend von der Norm ist nur die hier gewählte Auffassung und Formulirung der Sätze; doch wird man sich, wie ich hoffe, davon überzeugen, dass diese Theorie im Gewande der Dedekind'schen Anschauungen an Einfachheit und Durchsichtigkeit nur gewinnen kann. Auch ist die Einschränkung auf „Zahlen", die wir hier um

der zahlentheoretischen Ziele dieser Arbeit willen haben eintreten lassen, keineswegs eine wesentliche, und eine Erweiterung der Begriffe und Sätze auf „Functionen“ kann erheblichen Schwierigkeiten nicht unterliegen.

Wir wenden uns nunmehr nach Behandlung der rationalen Beziehungen überhaupt, welche zwischen derartigen Körpern von Zahlen bestehen, zur Untersuchung der entsprechenden Verhältnisse, welche für die ganzen Zahlen dieser Bereiche obwalten, d. h. zur Untersuchung entsprechender Beziehungen der Ideale. Der Kürze halber müssen wir hier ebensowohl die Dedekind'sche Begründung der Theorie der Ideale, wie die Theorie der Moduln, auf denen jene beruht, im wesentlichen als bekannt voraussetzen und uns darauf beschränken, mit wenigen einleitenden Worten an einige Hauptsätze dieser Theorie zu erinnern.

II.

Ideale.

14. Wenn eine derjenigen Gleichungen mit rationalen Coefficienten, welchen eine algebraische Zahl genügt, ganzzahlige Coefficienten und die Zahl 1 zum Coefficienten der höchsten Potenz hat, so heisst die Zahl eine algebraische ganze oder kurz eine ganze Zahl.*) Speciell muss die irreductibele Gleichung, welcher eine ganze Zahl genügt, wie man aus einem bekannten Satze von Gauss**) herleitet, eben die charakterisirte Eigenschaft haben, ganze rationale Zahlen zu haben, wenn man den Coefficienten der höchsten Potenz der Gleichung gleich 1 macht. Jede gebrochene algebraische Zahl kann durch Multiplication mit einer ganzen rationalen Zahl in eine ganze Zahl verwandelt werden, und die Gesammtheit dieser Zahlen bildet offenbar einen Modul, dessen Basis die kleinste von ihnen ist. Dieser Satz kann dahin verallgemeinert werden: Die Gesammtheit derjenigen ganzen Zahlen, welche in einem Körper Ω enthalten sind und welche die gegebene algebraische Zahl α durch Multiplication in eine ganze Zahl verwandeln, bildet ein Ideal des Körpers Ω; und dieser Satz könnte dann geradezu zur Definition des Ideals verwendet werden.

*) Die Begriffe der ganzen Zahl, ihrer Theilbarkeit und auch des grössten gemeinschaftlichen Theilers sind vom Begriffe des Körpers unabhängig.

**) Disqu. ar. 42.

Die Summe, die Differenz und das Product zweier ganzen Zahlen ist wieder eine ganze Zahl (D. § 160, B. § 13), und da man durch die genannten Operationen auch nicht aus einem Körper heraustritt, so bildet die Gesammtheit aller in einem Körper Ω enthaltenen ganzen Zahlen einen Modul, welcher zudem die Eigenschaft hat, dass seine Zahlen sich auch durch Multiplication reproduciren. Wir bezeichnen diesen Modul durch $\mathfrak{o}$ und nennen ihn die Hauptordnung des Körpers Ω. Die ganzen Zahlen besitzen aber zudem noch eine zweite Art der Reproduction, welche die ursprüngliche Definition der ganzen Zahl in einem allgemeineren Lichte erscheinen lässt: hat man eine algebraische Gleichung, in welcher der Coefficient der höchsten Potenz die Eins und die übrigen Coefficienten ganze algebraische Zahlen sind, so ist jede Wurzel dieser Gleichung eine ganze algebraische Zahl. Wir bezeichnen diese beiden Gesetze kurz als das erste und zweite Gesetz der Reproduction.

Wenn das Resultat der Division einer ganzen Zahl α durch eine ganze Zahl β eine ganze Zahl γ ist, so heisst α durch β theilbar. Dann folgt aus dem ersten Gesetze der Reproduction, dass die Grundgesetze der Theilbarkeit stattfinden: wenn α durch β und β durch γ, so ist α durch γ theilbar; und wenn α und β durch γ, so ist auch $\alpha \pm \beta$ durch γ theilbar. Aus dem zweiten Gesetze der Reproduction folgt aber, dass die Zerlegbarkeit der ganzen Zahlen im Gebiete aller algebraischen Zahlen eine unbeschränkte ist. Sobald man aber aus dem Gebiete eines bestimmten endlichen Körpers nicht heraustritt, dann ist zwar, wie man aus den Zahlenwerthen der Normen erkennt, die Zerlegbarkeit der ganzen Zahlen eine beschränkte, und die Principien der Zahlentheorie fangen an Platz zu greifen; während indessen im Gebiete der rationalen Zahlen und auch in einigen quadratischen Körpern*) die Eindeutigkeit der Zerlegbarkeit ohne

*) Diese quadratischen Körper lassen sich folgendermassen bezeichnen: Wird der Körper durch die von allen rationalen Factoren befreite Irrationalität $\sqrt{D}$ charakterisirt, so ist D entweder $\equiv \begin{matrix}2\\3\end{matrix}$ (mod. 4) oder $\equiv 1$ (mod. 4). Im ersten Falle bezeichnen wir die primitiven quadratischen Formen erster Art,

weiteres gesichert ist, kommen im Allgemeinen die Sätze, auf welche sich diese Eindeutigkeit stützt, in Wegfall, und dann ist die Einführung neuer Theorieen nothwendig.

Man kann nun, wie man leicht erkennt, als Basis des Körpers Ω vom Grade n (§ 3) stets n ganze Zahlen

$$\omega_1, \omega_2, \ldots \omega_n$$

wählen, und dann ist die Zahl

$$(1) \quad \omega = \Sigma_i x_i \omega_i \qquad i = 1, \ldots n$$

sicher eine ganze Zahl, wenn die Coordinaten x ganze rationale Zahlen sind, aber es kann im allgemeinen sehr wohl vorkommen, dass die Zahl ω ganz und die Coordinaten x gebrochene rationale Zahlen sind. Dann lässt sich aber zeigen, wenn k der Generalnenner der Brüche ist, dass die Discriminante

$$\Delta(\omega_1, \omega_2, \ldots \omega_n)$$

durch k^2 theilbar ist und dass man die Zahlen $\omega_1, \omega_2, \ldots \omega_n$ mit n neuen ganzen Zahlen $\omega_1', \omega_2', \ldots \omega_n'$ durch n Gleichungen mit rationalen Coefficienten:

$$(2) \quad \omega_i = \Sigma_k p_{ik} \omega_k' \qquad \begin{matrix} i \\ k \end{matrix} = 1, \ldots . n$$

so in Beziehung setzen kann, dass

$$(3) \quad \Delta(\omega_1, \omega_2, \ldots \omega_n) = k^2 \Delta(\omega_1', \omega_2', \ldots \omega_n')$$

ist; es ist also $\omega_1', \omega_2', \ldots \omega_n'$ eine neue ganzzahlige Basis des Körpers Ω, deren Discriminante kleiner als die alte ist. Denkt man sich also unter allen möglichen ganzzahligen Basen des Körpers Ω eine von denjenigen gewählt, deren Discriminante den kleinsten Werth hat, und bezeichnen wir diese jetzt durch $\omega_1, \omega_2, \ldots \omega_n$, so muss dieselbe die Eigenschaft haben, dass die durch die Gleichung (1) bestimmte Zahl α nur dann eine ganze Zahl ist, wenn die Coordinaten x ganze rationale Zahlen sind. Eine solche Basis heisst eine **Basis**

---

im zweiten Falle die primitiven quadratischen Formen zweiter Art der Determinante D als die entsprechenden quadratischen Formen des Körpers. Soll nun keine Einführung idealer Zahlen nothwendig sein, so muss

1. wenn die Determinante D positiv ist und die Gleichung $t^2 - Du^2 = -1$ keine Lösung hat, die Classenanzahl der entsprechenden quadratischen Formen = 2 sein.

2. In allen übrigen Fällen muss die Classenanzahl der entsprechenden quadratischen Formen = 1 sein.

der Hauptordnung des Körpers Ω; die Discriminante dieser Basis, deren wirkliche Berechnung im allgemeinen mit grossen Schwierigkeiten verbunden ist, heisst die Discriminante des Körpers Ω. Man erhält aus der Basis $\omega_1, \omega_2, \ldots \omega_n$ alle möglichen Basen der Hauptordnung durch Transformationsgleichungen der Form (2), wenn in ihnen der Absolutwerth der Determinante

$$\Sigma \pm p_{11}\, p_{22} \cdots p_{nn}$$

gleich Eins angenommen wird. Aber es ist wohl zu beachten, dass es keineswegs nothwendig ist, dass die Basis der Hauptordnung stets durch die n ersten Potenzen einer in $\mathfrak{o}$ enthaltenen Zahl Θ gebildet werden könne.

Ein in der Hauptordnung $\mathfrak{o}$ enthaltener Modul $\mathfrak{a}$, welcher die Eigenschaft besitzt, dass das Product einer Zahl von $\mathfrak{a}$ und irgend einer Zahl von $\mathfrak{o}$ wieder eine Zahl von $\mathfrak{a}$ ist, heisst ein Ideal. Da Ideale Moduln sind, so sind die Begriffe der Theilbarkeit, des grössten gemeinschaftlichen Theilers und des kleinsten gemeinschaftlichen Multiplums und der Multiplication ohne weiteres auf Ideale zu übertragen; dass aber die Begriffe der Theilbarkeit und der Multiplication der hier eingeführten Ideale sich decken, oder anders gesagt, dass ein Ideal $\mathfrak{a}$, welches ein Multiplum eines Ideals $\mathfrak{b}$ ist, auch das Product des Ideals $\mathfrak{b}$ und eines dritten Ideals $\mathfrak{c}$ ist, ist ein fundamentaler Satz dieser Theorie, welcher nur durch eine Kette recht complicirter Schlüsse zu beweisen ist. (D. §§ 168 — 173, B. §§ 19—25.)

Man erhält dies aus dem Satz:

Jedes Ideal lässt sich stets und nur auf eine Weise als ein Product von lauter Primidealen darstellen:

$$\mathfrak{a} = \mathfrak{p}^a\, \mathfrak{q}^b\, \mathfrak{r}^c \ldots,$$

und zwar ist

$$N(\mathfrak{a}) = N(\mathfrak{p})^a\, N(\mathfrak{q})^b\, N(\mathfrak{r})^c \ldots.$$

15. Betrachtet man nun die in einem Körper Ω enthaltene Gesammtheit von Idealen, so ist von besonderem Interesse für die Untersuchung das Verhältniss, in welches die Hauptideale des Körpers zu denjenigen Idealen treten, die nicht Hauptideale sind und die man wohl passend Nebenideale nennen

könnte. Jedes (Neben-)Ideal kann durch Multiplication mit einem passend gewählten Ideal in ein Hauptideal verwandelt werden, und dieser Multiplicator kann — was mitunter von Wichtigkeit ist — stets so gewählt werden, dass er relatives Primideal zu einem beliebig vorgegebenen Ideale $\mathfrak{b}$ wird. (D. §§ 174, 175; B. § 28). Hieraus folgt dann leicht, dass jedes (Neben)-Ideal als grösster gemeinschaftlicher Theiler zweier Hauptideale, und zwar auf unendlich viele Arten, dargestellt werden kann.

Wenn zwei Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ durch Multiplication mit einem und demselben Ideal $\mathfrak{m}$ in Hauptideale verwandelt werden können, so heissen sie aequivalent. Ist $\mathfrak{am} = \mathfrak{o}\mu$, $\mathfrak{a}'\mathfrak{m} = \mathfrak{o}\mu$, so ist $\mathfrak{a}\mu' = \mathfrak{a}'\mu$; es giebt also zwei Zahlen, so dass das Product der einen Zahl und des einen Ideals gleich dem Producte der anderen Zahl und des anderen Ideals ist; und umgekehrt, wenn zwei Zahlen dieser Beschaffenheit existiren, so sind die Ideale aequivalent. Alle Hauptideale sind einander aequivalent, und ein Hauptideal ist auch nur einem Hauptideale aequivalent.

Die Gesammtheit aller einander aequivalenter Ideale bildet eine Idealclasse, welche durch irgend eines der in ihr enthaltenen Ideale als Repräsentant vertreten werden kann. Eine dieser Classen ist stets durch die Gesammtheit aller Hauptideale gebildet; diese heisst die Hauptclasse $\mathfrak{H}$ und kann durch die Hauptordnung $\mathfrak{o}$ repräsentirt werden. Giebt es überhaupt Nebenideale, so erhalten wir weitere Classen; in jedem Falle ist aber die Anzahl dieser Classen h eine endliche, wie durch gewisse Ungleichungen zu erweisen ist.

Sind die Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ einerseits und $\mathfrak{b}$ und $\mathfrak{b}'$ andererseits einander aequivalent, so ist auch das Product $\mathfrak{ab}$ dem Producte $\mathfrak{a}'\mathfrak{b}'$ aequivalent. Wählt man also aus einer Idealclasse A der Reihe nach alle Ideale $\mathfrak{a}$ und aus einer Idealclasse B der Reihe nach alle Ideale $\mathfrak{b}$ und multiplicirt die $\mathfrak{a}$ mit den $\mathfrak{b}$, so erhält man, wenn auch nicht alle, so doch jedenfalls lauter Ideale $\mathfrak{c}$, welche einer einzigen Idealclasse C angehören; diese Idealclasse C heisst das Product der Classen A und B oder auch die aus den Classen A und B zusammengesetzte Classe. Auf diese symbolische Mul-

tiplication trifft, wie man leicht erkennt, nicht bloss das Gesetz der Associativität, sondern auch das Gesetz der Commutativität zu. Die Hauptclasse verhält sich bei dieser symbolischen Multiplication, wie die Zahl Eins bei der gewöhnlichen Multiplication. Zu jeder Classe gehört eine bestimmte (verschiedene oder gleiche) Classe A^{-1}, welche mit jener multiplicirt die Hauptclasse $\mathfrak{O}$ erzeugt; diese Classe A^{-1} heisst die inverse oder die entgegengesetzte Classe von A. Ein System von Idealclassen, welches die charakteristische Eigenschaft besitzt, dass das Product irgend zweier Classen des Systems wieder eine Classe des Systems ist, bildet eine Gruppe von Idealclassen. (Vgl. § 10.) Die einfachste Gruppe wird durch die Hauptclasse allein, die höchste durch alle Idealclassen gebildet; nächst der durch die Hauptclasse gebildeten Gruppe werden die einfachsten Gruppen durch die Potenzen einer einzigen Idealclasse erzeugt; die Ordnung r der durch die einzige Classe A constituirten Gruppe, d. i. der niedrigste positive Exponent, auf den die Classe A potenzirt werden muss, um die Hauptclasse zu erzeugen, mag der Exponent heissen, auf den sich die Classe A bezieht; die Hauptclasse ist also diejenige Classe, welche sich auf den Exponenten 1 bezieht. Da die Ordnung jeder Untergruppe ein Theiler der Ordnung derjenigen Gruppe ist, welche die Untergruppe enthält, so ist der Exponent r, auf den sich die Idealclasse A bezieht, ein Theiler der Classenanzahl h.*)

16. Es sei nun $\mathfrak{a}$ ein (Neben-)Ideal und r der Exponent, auf welchen sich die Classe A bezieht, welche durch $\mathfrak{a}$ repräsentirt werden kann, so ist $\mathfrak{a}^r$ ein Hauptideal:

$$(1) \quad \mathfrak{a}^r = o\mu;$$

stellt man nun neben diese symbolische Gleichung die wirkliche Gleichung:

---

*) Bildet man für alle möglichen hier auftretenden Exponenten r den Quotienten $\frac{h}{r}$, so wäre der kleinste dieser Quotienten der „exponens irregularitatis“ nach Gauss, Disqu. ar. 306, VII.

$$(2) \quad \alpha_0^r = \mu,$$

so erkennt man folgendes:

1) Ist α_0 eine beliebige unter den r Wurzeln der Gleichung (2), so ist es zunächst eine ganze Zahl nach dem zweiten Gesetze der Reproduction, und jede in dem Ideale enthaltene Zahl α ist durch α_0 theilbar; denn es ist α durch $\mathfrak{a}$, folglich α^r durch μ, und folglich α durch $\sqrt[r]{\mu} = \alpha_0$ theilbar.

2) Von der Zahl α_0 ist keine frühere als die r^{te} Potenz in dem Körper Ω enthalten; denn wäre

$$(3) \quad \alpha_0^{r'} = \mu',$$

wo $r' < r$ und μ' eine Zahl aus $\mathfrak{o}$ bedeutet, so könnte man offenbar annehmen, dass r' bereits der kleinste aller möglichen Exponenten e sei, welche die Eigenschaft haben, dass α_0^e einer Zahl des Körpers Ω gleich sei. Liegt nun r zwischen dem q fachen und dem $(q + 1)$ fachen von r':

$$r = qr' + r'' \; (0 \leqq r'' < r'),$$

so könnte man die Gleichung (3) in die q^{te} Potenz erheben, und da $r \geqq qr'$ ist, so erkennt man alsdann, dass die Zahl μ durch μ'^q theilbar und dass der Quotient, der ja auch eine Zahl von $\mathfrak{o}$ ist, gleich $\alpha_0^{r''}$ sein müsste, wo nun $r'' < r'$ ist; und das widerspricht unserer Annahme. Auf Grund eines Satzes, den man in den Lehrbüchern der Substitutionentheorie angegeben findet*), kann man diesen Satz auch dahin aussprechen:

Die Gleichung (2) ist in unserem Körper Ω irreductibel; doch hat er in dieser Form für uns keine principielle Bedeutung.

3) Wenn also $\mathfrak{a}$ ein Nebenideal, somit $r > 1$ ist, so gehört die Zahl α_0, die wir soeben eingeführt haben, dem Körper Ω nicht an; da aber die Zahlen des Ideals $\mathfrak{a}$ die gemeinsame Eigenschaft haben, sämmtlich durch α_0 theilbar zu sein, und da man umgekehrt auch leicht nachweisen kann, dass alle Zahlen der Hauptordnung $\mathfrak{o}$, welche durch die Zahl

*) Netto, l. c. § 190, C. Jordan, l. c. 418.

α_0 theilbar sind, eben das Ideal $\mathfrak{a}$ bilden*), da ferner die Eigenschaft der gemeinsamen Theilbarkeit das Wesen des Ideales noch etwas besser zu charakterisiren scheint, als die vorher definitorisch eingeführten Eigenschaften: so wird es gut sein, neben die wirklich in $\mathfrak{o}$ enthaltenen ganzen Zahlen neue Zahlen zu stellen, die dem Körper Ω als solchem nicht angehören und die man ideale Zahlen nennt. Zu jedem Ideal gehört eine ideale Zahl, und die Unbestimmtheit, die dadurch erwächst, dass α_0 als Wurzel einer Gleichung r^{ten} Grades r-deutig ist, ist darum unerheblich, weil ja doch die Zahl α_0 wenigstens bis auf Einheiten bestimmt ist; und bei Theilbarkeitsfragen — und auf solche kommt es jetzt allein an — spielen Einheiten keine Rolle; so ist ja auch die zu einem Hauptideal $\mathfrak{o}\mu$ gehörige Zahl μ immer nur bis auf eine (allerdings hier dem Körper Ω selbst angehörige) Einheit bestimmt. Eine solche zu einem Ideal gehörige Zahl α_0, welche die Eigenschaft hat, dass die Gesammtheit aller Zahlen des Ideals $\mathfrak{a}$ gleichbedeutend mit der Gesammtheit aller in $\mathfrak{o}$ enthaltenen, durch α_0 theilbaren Zahlen ist, nennen wir, mag sie nun wirklich oder ideal sein, die Charakteristik des Ideals. Die Charakteristik eines Primideals heisst eine (ideale oder wirkliche) Primzahl, die anderen Charakteristiken (ideale oder wirkliche) zusammengesetzte Zahlen, und unser früherer Hauptsatz lautet nunmehr so:

Jede in dem Körper Ω enthaltene ganze Zahl kann im wesentlichen nur auf eine Weise (d. h. abgesehen von Einheiten) als Product (idealer oder wirklicher) Primzahlen dargestellt werden.

Bestimmen wir nun die idealen Zahlen, welche in einem Körper Ω den wirklichen adjungirt werden müssen, damit die Gesetze der Theilbarkeit ausnahmslos Platz greifen, etwas genauer. Vorweg bemerken wir, dass zwischen idealen und wirklichen Zahlen des Gebietes $\mathfrak{o}$ jetzt kein Gegensatz mehr herrschen soll: wirkliche Zahlen sind eine specielle Art idealer

*) Denn wenn eine Zahl ω von $\mathfrak{o}$ durch α_0 theilbar ist, so ist ω^r durch $\alpha_0^r = \mu$ und folglich ω^r durch $\mathfrak{a}^r$, ω durch $\mathfrak{a}$ theilbar; d. h. ω ist eine Zahl von $\mathfrak{a}$.

Zahlen, und wenn wir von idealen Zahlen sprechen, so sind die wirklichen nicht mehr ausgeschlossen. Charakteristiken aequivalenter Ideale heissen aequivalente ideale Zahlen, und die Charakteristiken einer Classe von Idealen bilden eine Classe idealer Zahlen. Zunächst folgt sofort: das Product zweier idealer Zahlen des Körpers Ω ist wieder eine ideale Zahl des Körpers; denn sind die Zahlen α_0 und α_0' die Charakteristiken der Ideale $\mathfrak{a}$ und $\mathfrak{a}'$, so ist nach dem Vorhergehenden $\alpha_0\alpha_0'$ die Charakteristik des Ideals $\mathfrak{a}\mathfrak{a}'$. Der Multiplication der Ideale entspricht also vollkommen die Multiplication der Charakteristiken, so dass man, wenn man die Idealclassen und ihre Composition kennt, auch weiss, welcher Classe das Product zweier idealer Zahlen angehört. Also der Satz:

Durch Einführung der idealen Zahlen wird die symbolische Multiplication der Ideale in eine wirkliche Multiplication der idealen Zahlen verwandelt.

Speciell haben wir:

Das Product inverser idealer Zahlen ist eine wirkliche Zahl.

Haben wir ein (Neben-)Ideal $\mathfrak{a}$, welches der Classe A angehört, so bilden die in ihm enthaltenen Zahlen die Gesammtheit aller derjenigen wirklichen Zahlen, welche durch $\mathfrak{a}$ theilbar sind. Stellt man die Hauptideale, deren Charakteristiken die in $\mathfrak{a}$ enthaltenen Zahlen sind, der Reihe nach als Producte des Ideals $\mathfrak{a}$ und eines Ideals $\mathfrak{m}$ dar, so gehören die sämmtlichen Ideale $\mathfrak{m}$, die man auf diesem Wege erhält, einer und derselben Idealclasse, nämlich der inversen Classe von A, an; und man erhält auf diesem Wege offenbar auch alle Ideale der Classe A^{-1}; denn das Product irgend eines Ideales dieser Classe mit $\mathfrak{a}$ ist ein Hauptideal, dessen Charakteristik durch $\mathfrak{a}$ theilbar und folglich in $\mathfrak{a}$ enthalten ist. Geht man nun von den Idealen zu ihren Charakteristiken, den idealen Zahlen, über, so erkennt man auf Grund des eben Gesagten, dass die sämmtlichen idealen Zahlen einer Classe einen Modul bilden, welchen man erhält, wenn man die sämmtlichen in irgend einem Ideal $\mathfrak{a}$ der inversen Classe enthaltenen Zahlen durch die Charakteristik des Ideals $\mathfrak{a}$ dividirt; und da die

Basis des Ideals $\mathfrak{a}$ durch n in ihm enthaltene und von einander unabhängige Zahlen gebildet wird, so erhält man die Basis dieses Moduls, indem man die Basiszahlen des Ideals $\mathfrak{a}$ durch die Charakteristik des Ideals dividirt. Da zudem das Ideal $\mathfrak{a}$ die Eigenschaft hat, dass das Product irgend einer in ihm enthaltenen Zahl und einer Zahl der Hauptordnung $\mathfrak{o}$ wieder eine Zahl von $\mathfrak{a}$ ist, so muss der hier in Rede stehende Modul die Eigenschaft haben, dass irgend eine der in ihm enthaltenen idealen Zahlen, mit einer wirklichen Zahl multiplicirt, wieder eine ideale Zahl derselben Classe hervorbringt, eine Eigenschaft, welche wir schon vorher erkannt haben. Wir haben also den Satz:

Die Summe zweier aequivalenter idealer Zahlen ist eine ideale Zahl derselben Classe, oder jede Classe idealer Zahlen bildet einen Modul. Jedes Ideal der inversen Classe ist das Product dieses Moduls und seiner Charakteristik.

Man darf also ideale Zahlen beliebig multipliciren, und aequivalente ideale Zahlen darf man auch addiren und subtrahiren; aber nicht-aequivalente ideale Zahlen darf man nicht addiren und subtrahiren, wenn man nicht überflüssige d. h. solche Bildungen erhalten will, welche für die Untersuchung der Theilbarkeit der in einem endlichen Körper enthaltenen ganzen Zahlen keinen Werth haben. Bei der Addition und Subtraction aequivalenter idealer Zahlen ist aber noch auf eines zu achten: Die idealen Zahlen einer Classe A^{-1} bestimmten wir, indem wir von einem Ideale $\mathfrak{a}$ der inversen Classe A und der zugehörigen Charakteristik α_0 ausgingen; diese Charakteristik α_0 war nur bis auf gewisse, dem Körper Ω im allgemeinen nicht angehörige Einheiten bestimmt; nachdem aber einmal über α_0 eine Verfügung getroffen worden war, fanden wir für jedes Ideal der Classe A^{-1} eine bestimmte Charakteristik. Die Willkürlichkeit, welche sich uns bei Einführung der idealen Zahlen darbot, wird also sehr wesentlich beschränkt, wenn der Satz, dass aequivalente ideale Zahlen addirbar und subtrahirbar sind, keine Ausnahmen erleiden soll. Oder, wie man leicht erkennt, wenn man beachtet, dass inverse Classen sich auf denselben Expo-

nenten beziehen: Von einer Classe aequivalenter Zahlen ist nur eine einer gewissen Willkür unterworfen, wenn die Classe ein Modul sein soll.

17. Nach Einführung der idealen Zahlen stellten sich die einfachen Gesetze der Theilbarkeit, wie sie z. B. im Körper R der rationalen Zahlen herrschen, wieder her. Insbesondere gilt der Satz, der bekanntlich als Grundlage der Theorie angesehen werden kann: Wenn ein Product zweier wirklicher Zahlen durch eine ideale Primzahl π_0 theilbar ist, so ist wenigstens eine der beiden Zahlen durch π_0 theilbar. Es ist aber leicht zu sehen, dass derselbe Satz auch für zwei ideale Zahlen α_0 und β_0 (die wirklichen immer mit eingeschlossen) gilt: ist $\alpha_0\beta_0$ durch die Primzahl π_0 theilbar, so ist einer der beiden Factoren durch π_0 theilbar. Denn sind $\mathfrak{a}$, $\mathfrak{b}$ und $\mathfrak{p}$ die entsprechenden Ideale, so müsste, wenn der Satz falsch wäre, $\mathfrak{ab}$ durch $\mathfrak{p}$ theilbar, aber sowohl $\mathfrak{a}$ als $\mathfrak{b}$ zu $\mathfrak{p}$ relativ prim sein, und das ist unmöglich. Hieraus folgt in bekannter Weise, dass auch die idealen Zahlen sich in Beziehung auf Theilbarkeit ganz so wie die wirklichen Zahlen verhalten, nämlich im Wesentlichen nur eine Zerlegung in Primfactoren zulassen. Wir haben daher alle Veranlassung, die idealen Zahlen als gleichberechtigte Elemente bis zu einem gewissen Umfange in allen Theilbarkeitsfragen zuzulassen. Beginnen wir mit den Idealen selbst.

Die Gesammtheit aller in Ω enthaltenen ganzen Zahlen bildete das Ideal $\mathfrak{o}$ und die Einführung der idealen Zahlen können wir auch so charakterisiren: wir erweitern das Ideal $\mathfrak{o}$ um die idealen Zahlen (im ursprünglichen Sinne des Wortes). Es ist nun nur natürlich, alle Ideale in demselben Sinne zu vervollständigen; freilich wird hierdurch z. B. die einfache Eigenschaft verloren gehen, dass die Ideale Moduln sind; doch gewinnen wir dafür andere Vortheile. Ein Ideal $\mathfrak{a}$ war die Gesammtheit der durch die Charakteristik α_0 theilbaren wirklichen Zahlen der Hauptordnung $\mathfrak{o}$; unter dem vervollständigten Ideale $\mathfrak{a}$ verstehen wir die Gesammtheit aller durch α_0 theilbaren (wirklichen oder) idealen Zahlen. Ein vervollständigtes Ideal zerfällt in Classen, welche Moduln sind, von denen eine das Ideal ist, das vervollständigt wurde, und

und deren Composition mit der Multiplication der idealen Zahlen zugleich bekannt ist.

Wir gewinnen dadurch eine Begriffsbestimmung des grössten gemeinschaftlichen Theilers zweier idealer Zahlen α_0 und β_0, die uns bisher fehlte. Sind die entsprechenden Ideale $\mathfrak{a}$ und $\mathfrak{b}$ und ist ihr grösster gemeinschaftlicher Theiler das Ideal $\mathfrak{d}$, so definiren wir die Charakteristik des Ideales $\mathfrak{d}$ δ_0 als den grössten gemeinschaftlichen Theiler der Zahlen α_0 und β_0.*) In der That ist

$$\mathfrak{a} = \mathfrak{a}'\mathfrak{d} \qquad \mathfrak{b} = \mathfrak{b}'\mathfrak{d}, \text{ folglich}$$
$$\alpha_0 = \alpha_0'\delta_0 \qquad \beta_0 = \beta_0'\delta_0,$$

und jeder gemeinschaftliche Theiler von α_0 und β_0 muss ein Theiler von δ_0 sein, weil $\mathfrak{a}'$ und $\mathfrak{b}'$ relative Primideale sind. Wenn der grösste gemeinschaftliche Theiler zweier Zahlen eine Einheit ist, so heissen sie relative Primzahlen. Von Wichtigkeit ist es nun, dass wir mit Hilfe der Erweiterung der Ideale eine ebensolche Gleichung herleiten können, wie sie für den grössten Theiler d zweier rationaler Zahlen a und b besteht. Es seien nämlich $\overline{\mathfrak{a}}$ $\overline{\mathfrak{b}}$ und $\overline{\mathfrak{d}}$ die erweiterten Ideale und A, B und D die Classen, welchen die Zahlen α_0, β_0, δ_0 resp. angehören, so wählen wir aus dem Ideale $\overline{\mathfrak{a}}$ diejenige Classe aus, welche das Product der Zahl α_0 und der Zahlklasse DA^{-1} ist, und aus $\overline{\mathfrak{b}}$ diejenige Classe, welche das Product der Zahl β_0 und der Zahlclasse DB^{-1} ist. Diese beiden Classen der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ sind Moduln, deren Zahlen alle mit δ_0 aequivalent sind. Der grösste gemeinschaftliche Theiler beider Moduln ist eine Classe des vervollständigten Ideals $\overline{\mathfrak{d}}$, und diese ist keine andere als diejenige, welcher δ_0 angehört, denn durch Addition aequivalenter Zahlen erhält man eine Zahl derselben Classe. Folglich ist auf Grund des Begriffs des grössten gemeinschaftlichen Theilers zweier Moduln die in $\overline{\mathfrak{d}}$ enthaltene Zahl δ_0 die Summe aus einer Zahl der bezeichneten Classe des vervollständigten Ideals $\overline{\mathfrak{a}}$

*) Der Begriff des grössten gemeinschaftlichen Theilers zweier ganzer Zahlen ist, wie man mit Hilfe des § 6 erkennt, unabhängig vom Begriffe des Körpers.

und einer Zahl der bezeichneten Classe des vervollständigten Ideals $\overline{\mathfrak{b}}$:

$$(1)\quad \delta_0 = \alpha_0\xi_0 + \beta_0\eta_0;$$

wo die Zahlen ξ_0, η_0, resp. den Classen DA^{-1} und DB^{-1} angehören und die drei Zahlen δ_0, $\alpha_0\xi_0$, $\beta_0\eta_0$ einander aequivalent sind.

18. Gehen wir jetzt zu den Congruenzen über. Ist $\mathfrak{m}$ irgend ein Ideal von $\mathfrak{o}$, so kann die Congruenz

$$(2)\quad \alpha \equiv \beta \pmod{\mathfrak{m}},$$

wenn μ_0 die Charakteristik des Ideals $\mathfrak{m}$ ist, jetzt ohne weiteres ersetzt werden durch die Congruenz

$$(3)\quad \alpha \equiv \beta \pmod{\mu_0}.$$

Aber wir sind jetzt nicht mehr genöthigt, die Zahlen α und β als wirkliche Zahlen zu denken, sie können jetzt allgemein nach dem Vorhergehenden aequivalente ideale Zahlen sein. Die Norm der idealen Zahl μ_0 setzen wir einfach (bis auf ein Vorzeichen, zu dessen Bestimmung man von anderen Gesichtspunkten ausgehen muss,) gleich der Norm des Ideals $\mathfrak{m}$:

$$(4)\quad \pm N(\mu_0) = N(\mathfrak{m}) = (\mathfrak{o}, \mathfrak{m})$$

und dann haben wir jetzt den Satz:

In jeder Classe idealer Zahlen giebt es $(N(\mu_0))$ Zahlen, welche nach dem Modul μ_0 einander incongruent sind.

Ein solches System incongruenter Zahlen heisst ein Repräsentantensystem der Classe nach dem Modul μ_0. Jede Zahl der Classe ist nach dem Modul μ_0 einer und nur einer Zahl eines Repräsentantensystems congruent. Uebrigens folgt aus der Congruenz (3) die Gleichung

$$(5)\quad \alpha = \beta + \mu_0\tau_0,$$

in welcher τ_0 eine Zahl der Classe $M^{-1}B$ ist, wenn M die Classe von μ_0 und B die Classe von α und β bedeutet. Alle Zahlen, welche einer und derselben Zahl β nach μ_0 congruent (und ihr aequivalent) sind, haben nach (5) denselben grössten gemeinschaftlichen Theiler mit μ_0. Bezeichnen wir mit $\psi(\mu_0) = \psi(\mathfrak{m})$ die Anzahl derjenigen Zahlen eines Repräsentantensystems einer Classe nach dem Modul μ_0, welche zu μ_0 relativ

prim sind, so ist die Anzahl derjenigen Zahlen desselben Repräsentantensystems, welche mit μ_0 den grössten Theiler δ_0 haben, wenn $\mu_0' = \frac{\mu_0}{\delta_0}$ ist, gleich $\psi(\mu_0')$, und hieraus folgt die Gleichung

$$(6) \quad \Sigma_{\delta_0} \psi(\delta_0) = |N(\mu_0)|,$$

worin die Summe über alle nicht associirten Theiler der idealen Zahl μ_0 erstreckt ist. Nach einer bekannten Methode*) leitet man hieraus die folgende Form der Zahl $\psi(\mu_0)$ ab: sind $\pi_1, \pi_2, \ldots \pi_n$ die sämmtlichen nicht associirten idealen Primtheiler der Zahl μ_0, so ist

$$(7) \quad \psi(\pi_0) = |N(\mu_0)| \left(1 - \frac{1}{|N(\pi_1)|}\right) \left(1 - \frac{1}{|N(\pi_2)|}\right) \cdots \left(1 - \frac{1}{|N(\pi_n)|}\right),$$

und wenn also μ_0 eine ideale Primzahl π_0 ist, so ist

$$(8) \quad \psi(\pi_0) = |N(\pi_0)| - 1.$$

Aus der Form (7) folgt: Sind α_0 und β_0 relative Primzahlen, so ist

$$(9) \quad \psi(\alpha_0\beta_0) = \psi(\alpha_0)\, \psi(\beta_0).$$

Diesen letzten Satz erkennt man auch auf anderem Wege: Die lineare Congruenz:

$$(10) \quad \alpha_0 \xi \equiv \beta_0 \pmod{\mu_0}$$

ist dann und nur dann lösbar, wenn der grösste Theiler δ_0 von α_0 und μ_0 Theiler von β_0 ist; und wenn diese Bedingung erfüllt ist, so erhält man im ganzen $|N(\delta_0)|$ incongruente Zahlen ξ, die die Congruenz befriedigen und der Zahlclasse $A^{-1}B$ angehören, wenn A die Zahlclasse von α_0, B die Zahlclasse von β_0 bedeutet. Wenn also α_0 zu μ_0 relativ prim ist, hat die Congruenz (10) stets eine und nur eine Lösung incongruenter Zahlen. Hieraus folgt: Sind α_0 und β_0 aequivalente ideale Zahlen und μ_0 und ν_0 relative Primzahlen, so haben die Congruenzen

$$(11) \quad \xi \equiv \alpha_0 \pmod{\mu_0} \text{ und } \xi \equiv \beta_0 \pmod{\nu_0}$$

eine gemeinsame Lösung und zwar sind die sämmtlichen

*) Dedekind, Crelles Journal Bd. 54, S. 25.

Zahlen ξ einander nach dem Modul $\mu_0\nu_0$ congruent; und weiter:

Sind α_0 und β_0 zwei ideale Zahlen, welche den Classen A und B angehören, und durchläuft in dem Ausdrucke $\alpha_0\xi_0+\beta_0\eta_0=\sigma\ \xi_0$ ein Repräsentantensystem einer Classe X nach dem Modul β_0 und η_0 ein Repräsentantensystem einer Classe Y nach dem Modul α_0, so durchläuft, wenn

$$AX = BY$$

ist, σ ein Repräsentantensystem der Classe AX nach dem Modul $\alpha_0\beta_0$; und wenn ξ_0 bloss die $\psi(\beta_0)$ Zahlen des ersten Repräsentantensystems, welche zu β_0 relativ prim, und η_0 bloss die $\psi(\alpha_0)$ Zahlen des zweiten Repräsentantensystems durchläuft, welche zu α_0 relativ prim sind, so durchläuft σ bloss die $\psi(\alpha_0\beta_0)$ Zahlen des dritten Repräsentantensystems, welche zu $\alpha_0\beta_0$ prim sind. Der letzte Theil dieses Satzes spricht die Formel (9) aus.

Eine Congruenz n^{ten} Grades

(12) $\alpha_0\xi^n+\beta_0\xi^{n-1}+\gamma_0\xi^{n-2}+\ldots+\varkappa_0\xi+\lambda_0\equiv 0\ (\mathrm{mod.}\pi_0)$,

deren Modul π_0 eine ideale Primzahl und deren höchster Coefficient α_0 zu π_0 relativ prim sein soll, kann lösbar sein, wenn die Zahlclassen

$$A\ B\ C\ \ldots\ J\ K\ L,$$

denen die Coefficienten

$$\alpha_0\ \ \beta_0\ \ \gamma_0\ \ldots\ \iota_0\ \ \varkappa_0\ \ \lambda_0$$

zugehören, den Bedingungen genügen:

$$AL^{n-1}=K^n,\ \ BL^{n-2}=K^{n-1},\ \ldots,\ JL=K^2;$$

aber sie kann, wie leicht zu erweisen, nie mehr als n incongruente Wurzeln haben.

Wir wenden uns nun jetzt speciell zu den binomischen Congruenzen und zum allgemeinen Fermatschen und Wilsonschen Satze. Schliessen wir zunächst Moduln μ_0, welche zusammengesetzte ideale Zahlen sind, nicht aus, und ist α_0 eine beliebige ideale Zahl, welche zu μ_0 relativ prim ist, bezieht sich ferner die Classe A, welcher α_0 zugehört, auf den Exponenten r (§ 15), so bilden wir die Reihe der zu μ_0 relativ primen Zahlen:

$$1,\ \alpha_0,\ \alpha_0^2,\ \ldots\ \alpha_0^r,\ \alpha_0^{r+1},\ \ldots\ \alpha_0^{2r},\ \alpha_0^{2r+1}\ \ldots\ ,$$

so sind der Zahl 1, die ja zur Hauptclasse gehört, nur die Zahlen

$$\alpha_0^{r},\ \alpha_0^{2r},\ \alpha_0^{3r},\ \ldots$$

aequivalent. Da diese Reihe eine unendliche Menge von Zahlen enthält, die Anzahl der einander incongruenten Zahlen der Hauptclasse mod. μ_0 aber nur eine endliche ist, so folgert man in der üblichen Weise, dass es eine Zahl e geben muss, derart, dass

$$(13)\quad \alpha_0^{er} \equiv 1 \pmod{\mu_0}$$

ist, und dass, wenn e die kleinste aller positiven Zahlen ist, welche die Gleichung (13) erzeugen, die Potenzen

$$1,\ \alpha_0^{r},\ \alpha_0^{2r},\ \ldots\ \alpha_0^{(e-1)r}$$

einander incongruent sein müssen. Das mit dieser kleinsten Zahl e gebildete Product er mag der Exponent heissen, auf welchen sich die Zahl α_0 mod. μ_0 bezieht; dieser Exponent ist stets ein Vielfaches des Exponenten, auf welchen sich die Classe A von α_0 bezieht. Mit Hilfe der hier schon mehrfach angewendeten Exhaustionsmethode (Disqu. ar. 49, 83) schliesst man jetzt leicht, dass e stets ein Theiler von $\psi(\mu_0)$ sein muss, und folglich ist stets:

$$(14)\quad \alpha_0^{r\psi(\mu_0)} \equiv 1 \pmod{\mu_0};$$

d. i. das Fermatsche Theorem. Man erkennt übrigens, dass die Annahme, dass α_0 eine ideale Zahl ist, hier nicht eben wesentlich ist, weil α_0^{r} doch eine wirkliche Zahl α ist. Wir können also ohne Beschränkung der Allgemeinheit $r = 1$ und α_0 gleich einer wirklichen Zahl von o setzen, und dann haben wir:

$$(14')\quad \alpha^{\psi(\mu_0)} \equiv 1 \pmod{\mu_0}$$

Ist μ_0 gleich einer Potenz einer idealen Primzahl, $\mu_0 = \pi_0^{m}$, so ist $\psi(\mu_0) = |N(\pi_0)|^{m-1}\,(|N(\pi_0)|-1)$, also

$$(15)\quad \alpha^{|N(\pi_0)|^{m-1}\,(|N(\pi_0)|-1)} \equiv 1 \pmod{\pi_0^{m}}$$

und für $m = 1$

$$(16)\quad \alpha^{|N(\pi_0)|-1} \equiv 1 \pmod{\pi_0}$$

Multiplicirt man diese Gleichung mit α, so kann man die Annahme, dass α durch π_0 nicht theilbar sei, in Wegfall kommen lassen, es ist also für jede wirkliche Zahl α:

$$(16)\quad \alpha^{N(\pi_0)} \equiv \alpha \pmod{\pi_0}.$$

Die Congruenz

$$\xi^{N(\pi_0)-1} - 1 \equiv 0 \pmod{\pi_0}$$

hat also $|N(\pi_0)| - 1$ incongruente wirkliche Zahlen zu Wurzeln, und folglich besteht nach dem vorher genannten allgemeinen Fundamentalsatz über Congruenzen beliebig hoher Ordnung die in Beziehung auf ξ identische Congruenz:

$$(17)\quad \xi^{N(\pi_0)-1} - 1 \equiv \Pi_\varrho (\xi - \varrho) \pmod{\pi_0},$$

in welcher das Product auf der rechten Seite über ein System wirklicher Zahlen ϱ erstreckt ist, welche alle einander incongruent und alle zu π_0 relativ prim sind. Berücksichtigt man, dass $|N(\pi_0)| - 1 = \psi(\pi_0)$ gerade ist, wenn die durch die ideale Primzahl π_0 theilbare rationale Primzahl p von 2 verschieden ist, und dass, wenn $\psi(\pi_0) = 2^m - 1$, also ungerade ist,

$$-1 \equiv +1 \pmod{\pi_0}$$

ist, so erhält man aus der Formel (17) für $\xi = 0$ den allgemeinen Wilson'schen Satz:

$$(18)\quad \Pi_\varrho \varrho \equiv -1 \pmod{\pi_0},$$

eine Formel, in welcher natürlich das Product Π über dieselben Zahlen wie in (17) zu erstrecken ist. Modulo einer idealen Primzahl π_0 bezieht sich eine reelle Zahl α, welche zu π_0 relativ prim ist, auf einen Exponenten e, welcher jedenfalls ein Theiler von $\psi(\pi_0) = N(\pi_0) - 1$ ist; es fragt sich, ob umgekehrt zu jedem Theiler e von $\psi(\pi_0)$ wirkliche Zahlen α existiren, welche sich auf diesen Theiler als Exponenten mod. π_0 beziehen. Bezeichnen wir dann für den Augenblick die Anzahl der incongruenten wirklichen Zahlen, welche sich auf den Theiler e von $\psi(\pi_0)$ beziehen, mit $\varphi'(e)$, so ist $\varphi'(e)$ also entweder Null oder eine positive Zahl. Man weist nun leicht nach, dass $\varphi'(e)$, wenn es von Null verschieden ist, gleich $\varphi(e)$ sein muss, wobei $\varphi(e)$ die bekannte Zahl bedeutet, die die Anzahl der einander incongruenten und zu e relativ primen Zahlen angiebt. Nun ist offenbar:

$$\Sigma_e \varphi'(e) = \psi(\pi_0),$$

wenn die Summe über alle Theiler e von $\psi(\pi_0)$ erstreckt ist und da auch

$$\Sigma_e \varphi(e) = \psi(\pi_0)$$

ist, so muss, da $\varphi'(e) \leq \varphi(e)$ ist, nothwendig $\varphi'(e) = \varphi(e)$ sein. Wir haben also den Satz, dass sich auf den Theiler e von $\psi(\pi_0)$ $\varphi(e)$ incongruente wirkliche Zahlen beziehen; und wenn wir den Theiler $e = \psi(\pi_0)$ setzen, und den Begriff der primitiven Wurzeln einführen, so erhalten wir: Modulo einer idealen Primzahl π_0 giebt es $\varphi(\psi(\pi_0))$ primitive Wurzeln. Wir können also die Theorie der primitiven Wurzeln und die Theorie der Indices auf unsere binomischen Congruenzen Modulo einer idealen Primzahl anwenden, und mit ihrer Hilfe oder auch allein mit Benutzung des Fundamentalsatzes über Congruenzen, des Fermat'schen und des Wilson'schen Satzes erhalten wir schliesslich den Satz über die Auflösbarkeit der binomischen Congruenzen:

Die binomische Congruenz:

$$(19) \quad \xi^m \equiv \delta \pmod{\pi_0},$$

in welcher δ eine wirkliche Zahl der Hauptordnung o bedeutet, ist auflösbar oder nicht auflösbar, je nachdem der grösste Theiler d vom m und $\psi(\pi_0)$ Theiler des Index von δ ist oder nicht; oder was dasselbe besagt, je nachdem die Congruenz

$$(20) \quad \delta^{\frac{\psi(\pi_0)}{d}} \equiv 1 \pmod{\pi_0}$$

besteht oder nicht besteht; und wenn die Bedingung der Auflösbarkeit gesichert ist, so hat die Congruenz (19) d incongruente Wurzeln.

19. Wir haben bis jetzt nur die Ideale und die idealen Zahlen eines Körpers Ω betrachtet und die mit Ω zugleich entstehenden conjugirten Körper Ω', Ω'', ... $\Omega^{(n)}$ ausser Acht gelassen. Indem wir die im ersten Abschnitt auseinandergesetzte Theorie der Permutationen auf den Körper Ω anwenden, gelangen wir zur Bestimmung der conjugirten Ideale und der conjugirten idealen Zahlen. Wenn wir die Permutation $P^{(n)}$, durch welche der Körper Ω in den conjugirten Körper $\Omega^{(n)}$ übergeht, auf ein Ideal $\mathfrak{a}$ des Körpers Ω;

anwenden, so bildet das System $\mathfrak{a}^{(r)}$ der Bilder der Zahlen des Ideals $\mathfrak{a}$ ein Ideal des Körpers $\Omega^{(r)}$, denn da bei jeder Permutation die rationalen Beziehungen erhalten bleiben, so besitzt das System $\mathfrak{a}^{(r)}$ ebensowohl wie das System $\mathfrak{a}$ die beiden charakteristischen Eigenschaften des Ideals; und da die Permutation eine umkehrbar eindeutige Abbildung ist, so entspricht jedem Ideal $\mathfrak{a}$ ein und nur ein Ideal $\mathfrak{a}^{(r)}$. Wir haben also den Satz:

Durch die n Permutationen eines endlichen Körpers Ω des Grades n erhält man aus den Idealen des Körpers Ω alle Ideale der n conjugirten Körper.

Auf Grund der Erhaltung der rationalen Beziehungen erkennt man auch leicht, dass die Bilder aequivalenter Ideale aequivalent sind und dass conjugirte Ideale sich auf denselben Exponenten beziehen, wie sich denn überhaupt in conjugirten Körpern die charakteristischen Eigenschaften der Ideale ganz gleichmässig finden. Ist überdies der Körper ein Normalkörper, so enthält er mit einem Ideal auch alle seine conjugirten Ideale.

Was nun die Beziehung anbetrifft, in welcher ein Normalkörper zu einem seiner Divisoren steht, so haben wir gesehen (§ 12), dass diese Beziehung durch eine Untergruppe der Gruppe der Permutationen des Normalkörpers charakterisirt ist; und umgekehrt: wenn U eine hinreichend ausgedehnte Untergruppe der Gruppe der Permutationen eines Normalkörpers ist, so bildet die Gesammtheit der Zahlen, welche bei allen diesen Permutationen und nur bei den Permutationen der Untergruppe ungeändert bleiben, einen Divisor Ω des Normalkörpers N. Wendet man diese Untergruppe von Permutationen nur auf die ganzen Zahlen (der Hauptordnung n) des Normalkörpers N an, so erhält man in der Gesammtheit derjenigen Zahlen, welche bei allen diesen Permutationen ungeändert bleiben, die ganzen Zahlen (der Hauptordnung o) des Divisors Ω. Wendet man aber schliesslich die Permutationen der Untergruppe U nur auf ein Ideal $\mathfrak{a}_n$ der Hauptordnung n des Normalkörpers N an, so erhält man offenbar, wie aus dem Begriffe des Ideals und der Permutation mit Leichtigkeit folgt, in der Gesammtheit derjenigen Zahlen

des Ideals $\mathfrak{a}_n$, welche bei allen diesen Permutationen ungeändert bleiben ein Ideal $\mathfrak{a}_0$ des Divisors Ω; und umgekehrt erkennt man, dass auch jedes Ideal $\mathfrak{a}_0$ auf diesem Wege erzeugt werden kann. In der Untergruppe U der Gruppe der Permutationen eines Normalkörpers N hat man daher ein Mittel, um aus den Idealen des Normalkörpers N unmittelbar die Ideale des zugehörigen Divisors Ω von N herzuleiten; und wir haben daher den Satz:

Mit der vollständigen Bestimmung der Eigenschaften der Normalkörper ist nicht bloss die Theorie der Gleichungen (der algebraischen Zahlen überhaupt), sondern auch die Theorie der Ideale (der ganzen algebraischen Zahlen im speciellen) vollendet.

Inhalts-Verzeichniss.

Vita.

Natus sum, Georg Landsberg, Vratislaviae 30. I. anno h. s. 65, patre Bernhardo, matre Philippina e gente Buttermilch. Gymnasium frequentavi Elisabetanum, quod auspiciis Fickerti, deinde Paechii maxime florebat. Accepto maturitatis testimonio litteris philosophicis, imprimis mathematicis operam dare constitui ac primum quidem Vratislaviae, deinde Lipsiae, tunc rursus domi studiis incubui. Examen rigorosum 19. Dec. anni praecedentis praestiti. Scholas et exercitationes adii virorum illustrium: F. Auerbach, F. Cohn, Dyck, B. Erdmann, Freudenthal, Galle, Klein, A. Mayer, O. E. Meyer, C. Neumann, Poleck, Rosanes, Schroeter, Schur, Staude, L. Weber, Th. Weber, G. Wiedemann. Liceat mihi hoc loco omnibus his viris doctis, imprimis iis, quorum exercitationibus aut seminariis interesse mihi permissum erat, sincero animo maximas agere gratias.

Thesen.

1. Der Satz, dass die Zahlen der Form $2^{2^\nu} + 1$ Primzahlen seien, ist von Fermat nicht mit Sicherheit aufgestellt worden.

2. Der Begriff der gleichförmigen Bewegung ist in gewissem Umfange arbiträr.

3. In der Frage nach der Gauss'chen Auffassung der allgemeinen complexen Grössen mit mehr als zwei Haupteinheiten verdient die Ansicht Dedekind's vor der von Weierstrass den Vorzug.

4. Das Problem der Willensfreiheit führt nothwendig auf eine Antinomie.